UNIVERSIDAD POLITÉCNICA DE MADRID
ESCUELA UNIVERSITARIA DE INFORMÁTICA
Campus Sur. Ctra. de Valencia km. 7
28031 Madrid

POLITÉCNICA

# UNIVERSIDAD POLITÉCNICA DE MADRID

ESCUELA UNIVERSITARIA DE INFORMÁTICA

## PROYECTO DE FIN DE CARRERA

INTRODUCCIÓN A LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD BASADOS EN ISO 27001 Y DESARROLLO DE HERRAMIENTA DE SOPORTE A LA IMPLANTACION

**AUTOR**: Daniel Fernández Carravilla

**TUTOR**: Jorge Ramió Aguirre

**Histórico de control de cambios del Documento**

| REVISIÓN | FECHA | AUTOR (ES) | DESCRIPCIÓN |
|---|---|---|---|
| 1.0 | | Daniel Fernández Carravilla | Versión inicial |
| 1.2 | | Daniel Fernández Carravilla | - Adecuación de la portada.<br>- Corrección de errores y erratas.<br>- Referencias en ilustraciones.<br>- Ampliación del apartado del proceso de desarrollo: Metodología y estimación de esfuerzo y costes.<br>- Añadido apartado final de conclusiones. |
| 1.2.1 | | Daniel Fernández Carravilla | Cambios en el modelo de métricas de objetivos. |
| | | | |
| | | | |
| | | | |
| | | | |

# ÍNDICES

## ÍNDICE DE CONTENIDO

# ÍNDICE DE ILUSTRACIONES

# 1. INTRODUCCIÓN

## 1.1 RESUMEN

El presente proyecto presenta una introducción a los sistemas de gestión de la Seguridad de la Información (o SGSI) y describe el proceso de **desarrollo de una herramienta informática de soporte a la implantación de forma fácil, eficaz y eficiente de un SGSI** (se referirá a partir de ahora a esta herramienta como **Herramienta de Implantación y Seguimiento de SGSI o HIS-SGSI**) **según lo definido por el estándar ISO/IEC 27001:2005.**

## 1.2 ALCANCE

El alcance del documento cubre en primer lugar la descripción e introducción a todos los conceptos, procesos y metodologías estandarizadas orientadas a la gestión de la seguridad de la información y por tanto a los SGSI y cuyo soporte será el objetivo de la herramienta HIS-SGSI.

En segundo lugar el documento cubre el proceso de análisis y diseño de la herramienta basada en los estándares anteriores.

El documento no detalla del proceso de realización y despliegue de los estándares para la seguridad de la información descritos anteriormente y que soportará la herramienta HIS-SGSI.

Sin embargo en el documento se describirán estos procesos de manera general, así como las metodologías más comunes para la implantación del SGSI (especialmente ISO/IEC 27001:2005).

Esto permitirá cuantificar y comparar los requisitos de seguridad de la información que debe cubrir la organización mediante la implantación de las salvaguardas o controles adicionales necesarios para el cumplimiento de todos los requisitos, de manera que será este proceso de seguimiento y gestión de implantación el que se cubrirá mediante la herramienta HIS-SGSI.

## 1.3 ESTRUCTURA DEL DOCUMENTO

La estructura que seguirá el documento, será la siguiente:

- Capítulos 1 y 2: La presente introducción donde se realiza una exposición del problema y el objetivo del proyecto.
- Capítulo 3: Donde se describe el estado actual de la seguridad en SSII, la exposición de la necesidad de la herramienta y se describe el modelo de seguridad de la información.
- Capítulo 4: Donde se describe el SGSI como un proceso para alcanzar la mejora en la seguridad en SSII de la organización.
- Capítulo 5: Donde se describe el proceso de análisis de riesgos necesario para la implementación de un SGSI en la organización.

- Capítulo 6: Donde se describe el plan de desarrollo de la herramienta incluyendo las fases de análisis, diseño y desarrollo de la herramienta.
- Capítulo 7: Donde se exponen las conclusiones del desarrollo de la herramienta y los casos de éxito en entornos reales de la misma.
- Bibliografía y referencias utilizadas en la elaboración del documento.
- Un glosario de términos y abreviaturas: Los conceptos, abreviaturas y términos relativos a la seguridad de la información y que son utilizados en el presente documento se encuentran detallados en este apartado.
- Un anexo: Donde se expone el inventario de controles del estándar ISO 27002:2005.

# 2. OBJETIVO

El objetivo principal del proyecto será una introducción a los sistemas de gestión de la Seguridad de la Información (o SGSI) y el posterior proceso de desarrollo de una herramienta práctica y útil que presente las características necesarias para la gestión eficiente, sencilla y unificada de las principales actividades derivadas de la implantación de un Sistema de Gestión de la Seguridad de la Información.

La herramienta se basará fundamentalmente en los siguientes principios:

- Da soporte a la implantación de un SGSI basado en ISO/IEC 27001.2005.
- Implementación un ciclo de vida de mejora continua de Deming o PDCA de la seguridad de la información en la organización.
- Implantación y seguimiento del estado de las salvaguardas, medidas o controles de seguridad según lo definido por los estándares internacionales ISO/IEC 27001.2005 e ISO/IEC 27002.2005.
- Gestión de los niveles de madurez de la implantación de las salvaguardas y controles basándose en el Modelo de Madurez de la Capacidad (CMM).

Dicha herramienta por lo tanto, estará orientada a las tareas que requiera la puesta en marcha y mantenimiento del SGSI a la vez que se adaptará a las necesidades y características de cualquier organización y tendrá el objetivo de hacer sostenibles en el tiempo todas las iniciativas en materia de Gestión de Seguridad de la Información aplicables en la organización.

La posibilidad de disponer de una herramienta para facilitar los procesos de implantación de un SGSI surge de la necesidad de cubrir las necesidades de los consultores/auditores implicados en este tipo de proyectos. Las necesidades cubiertas mediante la herramienta HIS-SGSI serían las siguientes:

- Aportar una visión en todo momento del estado global de la seguridad de la información en la organización que facilite y justifique la toma de decisiones, así como permitir la visión de la evolución en el tiempo y la mejora de la seguridad de la información en la organización mediante un ciclo de mejora continua.
- Apoyar al cumplimiento con las normativas aplicables en materia de seguridad de la información.
- Seguir un criterio homogéneo en la evaluación de los controles y verificaciones de cumplimiento de las distintas organizaciones.
- Permitir tener centralizada y controlada toda la información relativa a los procesos de mejora de la seguridad de la información en la organización.
- Facilitar el proceso de mejora de la seguridad en los activos y sistemas de información de la organización a través de la reducción del riesgo y mediante la implantación de las salvaguardas aplicables.

- Permitir justificar y racionalizar la inversión en seguridad de la información.

De este modo una vez terminado el proceso de desarrollo se dispone de una herramienta propietaria aunque adaptable a la estructura normativa de cada organización y que suele ser licenciada como soporte adicional a un servicio de gestión de la seguridad contratado por la organización cliente.

# 3. ANÁLISIS DE LA SITUACIÓN ACTUAL

## 3.1 CONTEXTO DEL PROBLEMA

Partiendo de los estudios realizados en los últimos años relativos a las tendencias en materia de seguridad de la información se pueden obtener algunos datos relevantes sobre la importancia de la Seguridad de la Información en las organizaciones de cualquier tipo:

- Aproximadamente la mitad de las organizaciones encuestadas indica que ha sufrido al menos un incidente de seguridad de la información durante el último año. Muchos de estos incidentes son provocados por el propio personal interno de la organización, lo que hace ineficaces las medidas establecidas para proteger de los ataques procedentes del exterior.
- La falta de preparación y medios en las organizaciones para tratar los casos de incidentes de seguridad desemboca en que el daño causado por los ataques sea aún mayor y más amplio en el tiempo.
- El crecimiento de los ataques diseñados específicamente para atacar objetivos determinados, la difusión de kits y la automatización que permiten realizar ataques sofisticados y masivos a personas sin conocimientos tecnológicos elevados hace que el número de ataques crezca de manera enormemente significativa en los últimos años.

  En parte debido a lo expuesto se puede añadir que:

  - Un crecimiento de los ataques con motivación puramente económica y que conduce a una profesionalización de los atacantes, cada ver más organizados y con personal especializado en la búsqueda de brechas en la seguridad de los sistemas.
  - Aumenta el número de ataques Zero Day o de día Cero es decir, aquellos que se producen antes de que se haga pública la existencia de la debilidad explotada.
- Los ataques se vuelven más complejos abarcando el aprovechamiento de debilidades no sólo tecnológicas, sino también operativas, ingeniería social, herramientas especializadas…etc.
- Un volumen significativo de pérdidas económicas, de imagen, de oportunidades de negocio…etc., se deben a falta de políticas, procedimientos de definidos y falta de control sobre el acceso a la información y a los sistemas, por ejemplo el robo o la pérdida de soportes de información o el abuso de privilegios por parte de usuarios de sistemas de información.
- Además, debido a la tendencia creciente hacia una proliferación del modelo de negocio deslocalizado de las organizaciones el cual implica que los empleados puedan conectarse a los sistemas de información de la organización casi desde cualquier lugar o incluso que obligue que los empleados lleven consigo alguna parte o componente del sistema de información fuera de la infraestructura segura de la organización.

De todo lo anterior se deduce que los incidentes a la seguridad de la información son algo común en los últimos años y se producen cada vez con una frecuencia mayor.

Esto supone la necesidad de establecer una disciplina de seguridad que proteja no sólo de las vulnerabilidades o debilidades conocidas, sino también de prevenir aquellas que sean posibles aunque sean desconocidas. Así mismo, supone la necesidad de reaccionar con rapidez y eficacia ante la publicación de nuevas vulnerabilidades, puesto que podrían empezar a ser explotadas en cualquier momento.

Por todo lo anterior existe la necesidad de dar un enfoque global para afrontar el tema de la seguridad a que debe abordar los siguientes problemas:

- **Concienciar a los usuarios acerca de los problemas de seguridad**
- **Seguridad lógica**, es decir, la seguridad a nivel de los datos, en especial los datos de la empresa, las aplicaciones e incluso los sistemas operativos de las compañías.
- **Seguridad en las telecomunicaciones: tecnologías de red, servidores de compañías, redes de acceso, etc.**
- **Seguridad física**, o *la seguridad de infraestructuras materiales*: asegurar las habitaciones, los lugares abiertos al público, las áreas comunes de la compañía, las estaciones de trabajo de los empleados, etc.

Por otro lado, la falta de coordinación y gestión de los esfuerzos para gestionar la seguridad tienen un efecto negativo en el negocio y reducen la eficiencia de las operaciones y del personal técnico. Por ello se necesitan herramientas de gestión que faciliten y automaticen los procesos necesarios para la toma de decisiones a nivel directivo basadas en la gestión de riesgos, el cumplimiento normativo y la coordinación de las auditorías, por nombrar algunos. De este modo las organizaciones pueden reducir el esfuerzo en estas tareas e invertirlo en actividades de mejora e innovación.

## 3.2 INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN

Según el estándar internacional ISO/IEC 27001:2005, la información, en todas sus formas (automatizada o no automatizada, formalizada o no formalizada, pública o reservada, etc.), es uno de los principales activos de cualquier organización, es necesaria para el normal funcionamiento y la consecución de los objetivos que tenga marcados y en consecuencia debe ser protegida adecuadamente.

Debido a esa importancia, las organizaciones necesitan proteger su información para asegurar que esté disponible cuando se necesite, que sea fiable y que su distribución esté controlada. Esta necesidad se ve agravada por el hecho de que la cantidad de información que maneja una organización y su complejidad crece de forma exponencial, dificultando los esfuerzos para su protección.

La situación descrita en el apartado anterior obliga a las organizaciones a establecer una disciplina que defina y gestione las variables, los procesos y los objetivos que intervienen el curso de cumplir con los requisitos o necesidades de seguridad establecidos como aceptables para cualquier organización.

## 3.3 MODELO DE SEGURIDAD DE LA INFORMACIÓN

Para la gestión de la seguridad de la información es habitual establecer o adoptar un modelo de la seguridad de la información partiendo de la información como activo central.

En este modelo se identificarán tanto los principios básicos que determinan la necesidad del nivel de seguridad en información como los actores que afectan a su estado tanto positivamente como negativamente.

Existen varios modelos para estimar el estado de la seguridad de la información, sin embargo el más extendido está basado en los principios básicos de **Confidencialidad**, **Integridad** y **Disponibilidad** que se detallarán en los apartados siguientes.

### 3.3.1 Principios básicos en la seguridad de la información

Dado que el nivel de seguridad de la información es algo abstracto, normalmente se aborda, por lo general, a través de los requisitos o grado de necesidad en la organización de los siguientes parámetros o principios básicos de acuerdo a la naturaleza de la información:

- **Confidencialidad**: Este principio permite asegurar que los individuos solamente tienen acceso a los recursos e información a los que están explícitamente autorizados.
  Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito a ser transmitida desde el comprador al comerciante y el comerciante de a una red de procesamiento de transacciones. Si una parte no autorizada obtiene el número de la tarjeta en modo alguno, se habrá producido una violación de la confidencialidad.
- **Integridad**: Este principio garantizará que la información del sistema estará disponible tal y como se almacenó y que se controla cualquier modificación no autorizada.
  La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con intencionalidad) modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La comprobación integridad de un mensaje se puede obtener mediante distintos métodos, uno de los más habituales suele realizarse mediante la obtención de un conjunto de datos auxiliar que permita la comprobación de la integridad como puede ser la firma digital.
- **Disponibilidad**: Este principio garantizará que los recursos de los activos de información y la información se encontrarán disponibles cuando sean necesarios para una entidad autorizada.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información los controles de seguridad deben asegurar tanto la disponibilidad de la información, los propios sistemas y los canales de comunicación, evitando interrupciones del servicio debido a incidentes causado por las causas más diversas como cortes de energía, fallos de hardware, software malicioso, actualizaciones del sistema…etc.

Cualquier hecho o incidente que afecte a cualquiera de estos principios pone en riesgo la seguridad de la información y por lo tanto puede afectar a los procesos de negocio de la organización degradando su normal funcionamiento y afectado a la productividad de la organización.

Por el contrario cualquier acción orientada a mejorar la eficiencia de cualquiera de las componentes minimizará la posibilidad de que se produzca un incidente que afecte al desarrollo normal del negocio mejorando el estado de la seguridad de la información, este es el principio que busca la el proceso de gestión de la seguridad de la información.


**Ilustración 1: Principios básicos de la seguridad de la información**

(Fuente: http://pedrochujutallicruz.blogspot.com.es/2010/07/principios-basicos-de-la-seguridad-de.html)

### 3.3.2 La seguridad de la información como servicio

Adicionalmente los estándares ISO-7498-2 e ITU-T X.800 para la interconexión abierta entre sistemas de información, definen los anteriores principios como parte del servicio de Seguridad que se ofrece como capa de servicio desde el punto de vista de las telecomunicaciones y la interconexión entre sistemas. Además añade los siguientes componentes del servicio de seguridad que complementan a los anteriores y que son interesantes a tener en cuenta, especialmente en la actualidad dado que las telecomunicaciones y el acceso global a las redes de información son la base de funcionamiento de numerosos sistemas de información.

- **Autenticidad (o Autenticación)**: Permite garantizar la identidad de los usuarios de los activos y recursos de información. Está relacionada con el principio de confidencialidad.
- **Control de acceso**: El servicio de control de acceso evita el uso no autorizado de los recursos. Este servicio controla quien puede tener acceso a un recurso, bajo qué condiciones puede tener lugar el acceso y qué operaciones se permiten hacer a aquel que accede a un recurso. De mismo modo que el anterior está relacionada con el principio de confidencialidad.
- **No repudio o evitar el rechazo**: El no repudio o irrenunciabilidad evita que las entidades pares que se comunican puedan denegar el haber participado en parte o en toda la comunicación. La definición según la recomendación X.509 de la UIT-T: Servicio que suministra la prueba de la integridad y del origen de los datos ambos en una relación infalsificable que pueden ser verificados por un tercero en cualquier momento. Está relacionada con el principio de integridad.

  Existen dos modalidades.
  - No repudio con prueba de origen.
  - No repudio con prueba de destino.

## 3.4 LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

### 3.4.1 Actores implicados en la seguridad de la información

Los actores implicados en la seguridad de la información los activos de información y todas aquellas entidades y circunstancias que de manera activa o pasiva pueden afectar de manera positiva o negativa a cualquiera de los principios de la seguridad de los activos de información de la organización descritos anteriormente.

Los actores más habituales suelen ser los siguientes:

- La **información** y **los recursos de información** son los **activos** principales de cualquier organización y por tanto el objetivo a proteger mediante la implantación de las acciones adecuadas que provean del nivel de seguridad adecuada a las necesidades de la organización y conforme a la naturaleza de la información.

- Las **amenazas** representan el tipo de acción que puede ser potencialmente dañina y se materializan en incidentes de seguridad que afectan a cualquier variable de la seguridad de la información y que por lo tanto como se verá en el punto siguiente pueden afectar a los principios básicos de integridad confidencialidad, disponibilidad o no rechazo necesarios.
- Las **vulnerabilidades** representan el grado de exposición a las amenazas de un activo de información particular en un contexto determinado.
- **Los controles o salvaguardas** representan todas las acciones que deben implementarse en la organización y tienen el objetivo de prevenir, contrarrestar o minimizar los riesgos sobre la seguridad y mejorar la protección ante las amenazas. Las salvaguardas que deberán implementarse en la organización pueden ser tanto soluciones técnicas como medidas de concienciación y capacitación por parte de los de usuarios de los activos de información de las reglas de seguridad definidas.

  De acuerdo a su naturaleza los controles pueden ser:
  - **Controles procedimentales o administrativos:** Políticas, procedimientos, leyes, regulaciones, políticas, guías, estándares...etc.
  - **Controles físicos**: Puertas, cierres, detectores de incendios, extintores…etc.
  - **Controles técnicos o lógicos:** Mecanismos de autenticación y control de acceso, antivirus, firewalls…etc.

  Los controles al respecto de su aplicación ante la ocurrencia de un incidente de seguridad pueden ser:
  - **Controles preventivos**: Previenen la posibilidad de ocurrencia de un incidente de seguridad antes de que se materialice. Los **controles disuasorios** son un tipo especial de controles preventivos diseñados para hacer desistir a un potencial atacante antes de que se produzca el ataque.
  - **Controles detectivos**: Identifican que se está produciendo un incidente de seguridad en la organización y aportar toda información posible relativa al mismo. En algunos casos este tipo de controles también aplican medidas correctivas.
  - **Controles correctivos**: Limitan y en ciertos casos corrigen la extensión del daño producido por el incidente de seguridad. Los **controles mitigantes** son un tipo de controles correctivos que además puede cubrir las deficiencias de otros controles.

Teniendo en cuenta los actores y sus relaciones descritas anteriormente podríamos estimar **el riesgo como el grado de exposición de un activo de la organización a que una amenaza se materialice en un incidente que afecte al activo de información, impactando con mayor o menor gravedad a los principios básicos de la seguridad de la información** (Confidencialidad, Integridad, Disponibilidad) lo que se traduciría en perjuicios a la organización.

El siguiente diagrama muestra las relaciones entre los actores descritos: activos, amenazas, vulnerabilidades y controles o salvaguardas. .

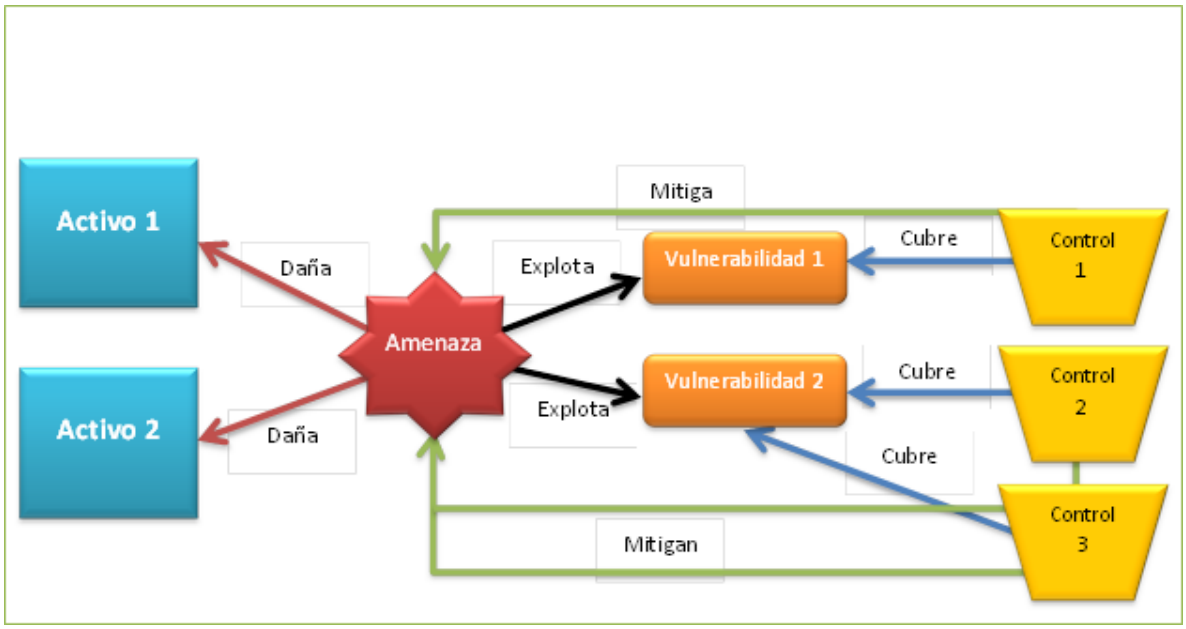



**Ilustración 2: Modelo de la seguridad de la información**

(Basado en: http://blog.patriot-tech.com/blog/bid/51353/An-Introduction-to-IT-Risk-Management)

Por todo lo anterior es fácil comprender que el riesgo es la variable principal a minimizar en toda gestión de la seguridad de la información, de modo que el objetivo de cualquier organización siempre será buscar su reducción al mínimo posible mediante la implantación de las correspondientes medidas o salvaguardas de seguridad.

Otro modelo con las entidades descritas y sus relaciones centrado en el riesgo y que también que incluiría otros conceptos como los impactos y las necesidades de seguridad de la organización.


**Ilustración 3: Modelo de la seguridad de la información centrado en el riesgo**

(Fuente: http://www.iso27000.es)

El riesgo suele estar ponderado de acuerdo al valor del activo para la organización, de modo que se podría aproximar de manera general mediante la siguiente ecuación:

$$\text{Riesgo} = \frac{\text{Amenazas} \times \text{Vulnerabilidades} \times \text{Valor del activo}}{\text{Controles}}$$

Para entender el concepto de riesgo mejor pensemos en el caso de un trapecista que quiere cruzar un foso con un cocodrilo mediante una cuerda.

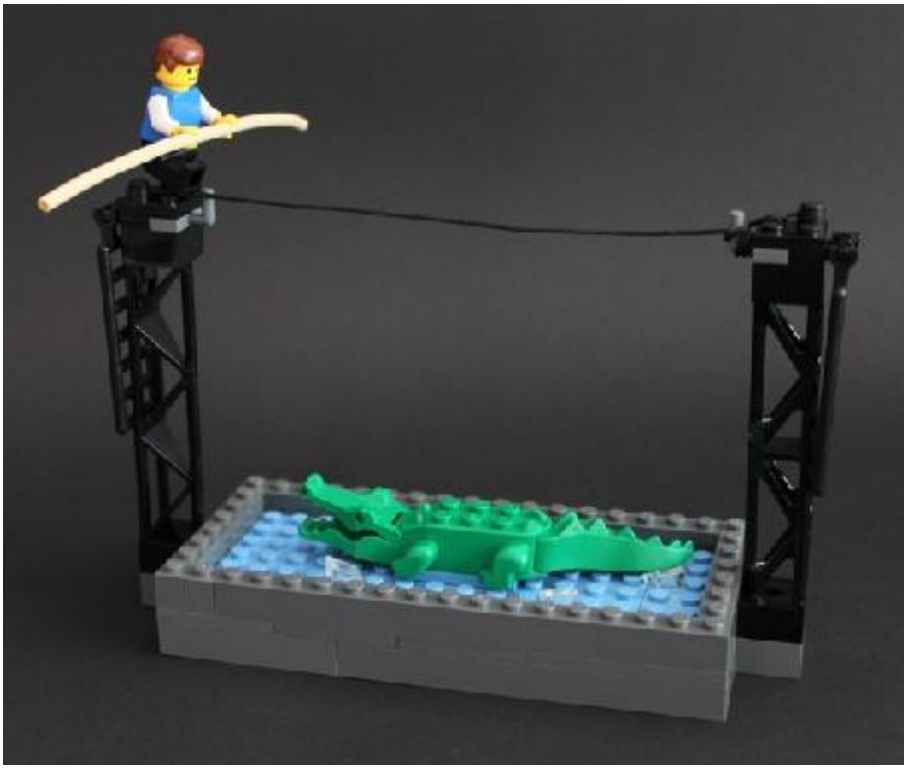


Ilustración 4: Ejemplo del modelo de riesgo

El **activo** que se quiere preservar es la integridad física del propio trapecista, algo por tanto muy valioso. La **amenaza** es la posibilidad de caída al foso del cocodrilo, la **vulnerabilidad** sería la circunstancia de falta de equilibrio del trapecista y el **riesgo** es el de sufrir daños de diversa consideración o incluso morir en caso de materializarse la caída. Para minimizar el riesgo que sufre el trapecista se implantaría una **salvaguarda**, (en este caso una red) que evitase que fuese devorado en caso de caída de la cuerda.

### 3.4.2 La gestión de la seguridad en las organizaciones

A partir del modelo expuesto anteriormente, podríamos definir la Gestión de la Seguridad como: **El proceso por el cual la organización define, alcanza y mantiene unos niveles apropiados de los componentes de la seguridad (Confidencialidad, Integridad y Disponibilidad) minimizando a la vez los riesgos a la seguridad de la información que pudieran afectarle y controlando y asegurando la accesibilidad a la información que necesita para operar.**

Por lo tanto de manera general cualquier proceso que persiga mejorar la seguridad de la información en la organización incluye las siguientes tareas:

1. Identificar las posibles amenazas y vulnerabilidades que pudieran afectar a los activos de información de la organización.
2. Determinar el riesgo potencial materialización de estas amenazas determinando la posibilidad de ocurrencia y el posible impacto en su caso.
3. Aplicar las medidas o salvaguardas adecuadas que anulen o minimicen la posibilidad de materialización de incidentes y por lo tanto del nivel riesgo.

De lo anterior se puede deducir que la correcta Gestión de la Seguridad de la Información se basa principalmente en el establecimiento y mantenimiento de planes de implantación de controles, salvaguardas y políticas, que tengan como finalidad conservar los principios de confidencialidad, integridad y disponibilidad de la información, es decir que tengan como objetivo lograr la seguridad de la información.

De este modo es habitual que las salvaguardas, controles o mecanismos de seguridad se implanten mediante proyectos que desplieguen los servicios o arquitecturas de seguridad adecuados que cubran las necesidades de seguridad de la información de la organización expuestas en sus Políticas de Seguridad.

La gestión de la seguridad de la información es por lo tanto hoy en día una parte fundamental de las organizaciones, con independencia de su tamaño, sector o localización geográfica.

Es por ello que una inadecuada gestión puede resultar en la materialización de las amenazas potenciales, incurrir en incumplimientos que resulten en sanciones, impactar en el desarrollo o la imagen del negocio y en muchos casos, el costo de la reparación puede superar el costo percibido de la prevención.

Particularizando y extendiendo el proceso de gestión de la seguridad según lo definido en la metodología MAGERIT 2006 (que se describirá más adelante) el proceso completo de Gestión de la Seguridad de la Información en las organizaciones incluye, entre otros, las siguientes actividades principales (aunque es muy similar en otras metodologías de gestión de la seguridad como ISO 27001):

- Determinar los objetivos, estrategias y políticas de Seguridad de la Información.
- Determinar los requisitos de Seguridad de la Información.
- Identificar y analizar las amenazas y las vulnerabilidades de los Activos de Información.
- Identificar y analizar los riesgos de seguridad.
- Especificar salvaguardas adecuadas teniendo en cuenta las amenazas, vulnerabilidades y riesgos identificados.

- Supervisar la implementación y el funcionamiento de las salvaguardas especificadas.
- Asegurar la concienciación de todo el personal en materia de Seguridad de la Información.
- Detectar los posibles incidentes de seguridad y reaccionar ante ellos.

Por ello el enfoque global y de negocio de la Seguridad de la Información requiere de herramientas de gestión capaces de facilitar a los responsables de la organización la toma de decisiones.

Entre estas herramientas de gestión destacaremos dos:

- El **análisis de riesgos** que permite identificar y valorar cuáles son aquellas amenazas más relevantes para la seguridad de la información desde un punto de vista de negocio y la eficacia de las salvaguardas establecidas para mitigar los riesgos asociados. Existen muchas metodologías comúnmente extendidas para el desarrollo de un análisis de riesgos como por ejemplo MAGERIT e ISO/IEC 27005.2008
- El **Sistema de Gestión de Seguridad de la Información (SGSI)** que consta de todos los elementos necesarios para planificar, definir, implantar, verificar y supervisar las medidas de seguridad necesarias para cumplir los requisitos de seguridad de la organización. El estándar más extendido para la definición e implantación de un SGSI es el ISO/IEC 27001.2005 que será el utilizado en el presente proyecto.

# 4. SISTEMA DE GESTIÓN DE LA SEGURIDAD

**Un Sistema de Gestión de Seguridad de la Información (SGSI) es el conjunto de políticas y procesos que permiten gestionar eficazmente todas las mejoras que se emprendan en la organización en materia de seguridad de la información y consta de todos los elementos necesarios para planificar, definir, implantar, verificar y supervisar las medidas de seguridad necesarias para cumplir los requisitos de seguridad de la organización.**

Por tanto un Sistema de Gestión de Seguridad de la Información comprenderá el diseño, implantación y mantenimiento de un conjunto de procesos que permitan gestionar eficientemente la accesibilidad de la información, buscando asegurar y mantener los niveles de confidencialidad, integridad y disponibilidad de los activos de información y minimizando a la vez los riesgos de seguridad de la información.

Normalmente la necesidad de establecer un SGSI parte desde un Plan Director de Seguridad de la Información cuyo desarrollo se debe definir como parte del Plan Estratégico Corporativo de cualquier organización.

El estándar más extendido para la definición e implantación de un SGSI es el ISO/IEC 27001:2005 y será el marco de referencia para el desarrollo de la herramienta HIS-SGSI.

## 4.1 EL ESTÁNDAR ISO 27001

Este estándar internacional ampliamente difundido plantea la seguridad en sistemas de información como un sistema de gestión compuesto de un conjunto de actuaciones a realizar en la organización, organizadas en un proceso de mejora continuo y con el objetivo de alcanzar el nivel de madurez deseado en la seguridad de la información de la organización.

El estándar internacional ISO/IEC 27001:2005 fue aprobado y publicado como estándar internacional en octubre de 2005 por la Organización Internacional para la Estandarización o OSI (International Organization for Standardization) y por la Comisión International Electrotécnica o IEC (International Electrotechnical Commission).

Tiene su origen en la norma BS7799, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI):

- La primera parte de esta normativa incluía un catálogo de buenas prácticas y evolucionará como ISO/IEC 17799 hasta finalmente llegar a ser ISO/IEC 27002 y en España como UNE/ISO-IEC27002:2005

- La segunda parte BS 7799-2 describía la implantación sistema de gestión de la seguridad que llegaría a ser ISO/IEC 27001:2005 que en España este estándar está reconocido por la UNE como UNE-ISO/IEC 27001. Es esta segunda parte la que utilizaremos como base en el presente documento, sin embargo la primera parte se utilizará como catálogo de medidas o controles de seguridad como se verá posteriormente.

Aunque no es obligatorio, es posible que la organización pueda certificar un SGSI según la norma ISO/IEC 27001, lo que puede aportar las siguientes ventajas a la organización:

- Demuestra implantación de los controles internos, cumple los requisitos de gestión corporativa y de continuidad de la actividad corporativa.
- Demuestra independientemente concienciación sobre las leyes y normativas que sean de aplicación. Proporciona una ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial.
- Verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información.
- Demuestra el compromiso de la cúpula directiva de su organización con la seguridad de la información.
- El proceso de evaluaciones periódicas ayuda a supervisar continuamente el rendimiento y la mejora.

Un SGSI conforme con el estándar ISO/IEC 27001:2005 constará fundamentalmente, de los siguientes elementos:

- **El análisis de riesgos**: Que determine el nivel de riesgo al que están expuestos los activos de información de la organización.
- **Un cuerpo normativo**, incluyendo:
    - Definición del alcance del SGSI.
    - Política de seguridad.
    - Declaración de aplicabilidad, que detalla los controles necesarios para alcanzar los objetivos de seguridad fijados.
    - Procesos de seguridad.
    - Procedimientos de seguridad.
    - Registros de seguridad.
- **Asignación de funciones y responsabilidades:**

Los procesos del SGSI se basan en la aplicación del Ciclo de Deming de PDCA (PDCA: Plan – Do – Check – Act), o de mejora continua aplicada en el ámbito de la seguridad de la información:


**Ilustración 5: Ciclo de Deming**

(Fuente: http://marcexchange.blogspot.com.es/2009/01/normas-iso.html)



- **Planifica (PLAN)**: Establecer los objetivos, políticas, normas, procesos, procedimientos necesarios para gestionar los riesgos y mejorar la seguridad de la información, de acuerdo a las necesidades y requisitos de la organización. (ISO/IEC 27001:2005 4.2.1b / 4.2.1g)
- **Hacer (DO)**: Definir e implantar y operar las políticas, procesos, procedimientos y controles definidos. (ISO/IEC 27001:2005 4.2.2d)
- **Verificar (CHECK)**: Evaluar la eficacia y eficiencia de las políticas, procesos, procedimientos y controles para lograr los objetivos de seguridad de la información definidos. Identificar aquellas no conformidades con la planificación realizada. (ISO/IEC 27001:2005 4.2.3c)
- **Actuar (ACT)**: Gestionar las medidas preventivas y correctivas destinadas a solucionar las no conformidades detectadas en la fase anterior, a mejorar el cumplimiento de los requisitos de seguridad de la información definidos y adaptar el sistema a los cambios internos y externos relevantes. El resultado de esta fase servirá para alimentar un nuevo Ciclo de Deming. (ISO/IEC 27001:2005 4.2.4d)

Todo el ciclo completo se puede definir en un proceso completo con sus entradas y salidas como el mostrado en el diagrama que se presenta a continuación y que se detallará en los apartados correspondientes que se detallarán en los puntos siguientes.

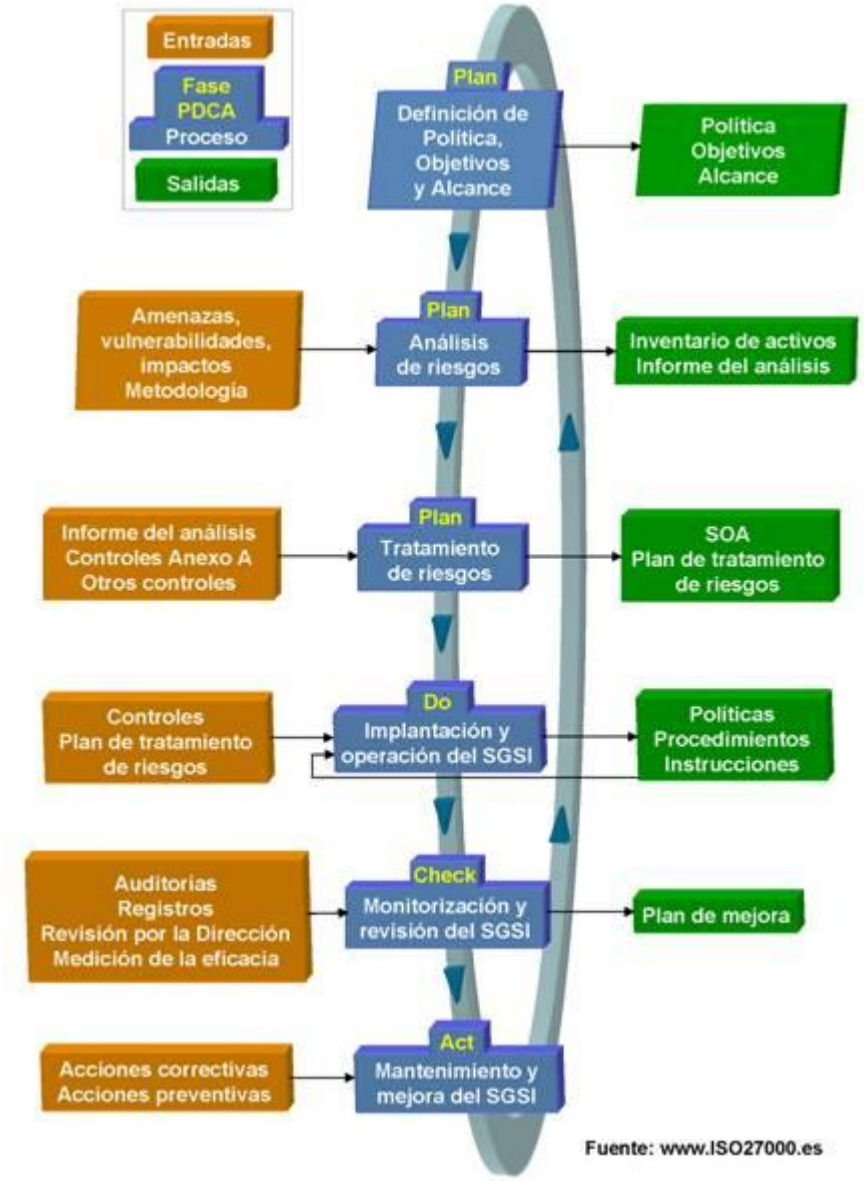



**Ilustración 6: Ciclo de Deming detallado**

(Fuente: http://www.iso27000.es)

## 4.2 FASE 1: PLANIFICAR - Planear la implantación del SGSI

### 4.2.1 Establecer el alcance y los objetivos del SGSI

En el primer paso se debe determinar el alcance del SGSI, es decir qué parte de la organización va a ser objetivo del SGSI, por ejemplo de entre los siguientes:

- Procesos
- Activos
- Tecnología
- Servicios

- Personal y relaciones con terceros

Es posible afrontar la organización completa, pero es perfectamente válido y muy recomendable en caso de organizaciones con poca experiencia en la gestión de la seguridad, comenzar por un área determinada de la organización o conjunto de procesos que sean relevantes o especialmente sensibles para el negocio, por ejemplo, en el caso de una compañía con posibilidad de venta online podría ser el proceso de venta a través de la Web.

En segundo lugar uno de los aspectos más importantes en el proceso de construcción de un SGSI es el establecimiento de los Objetivos Estratégicos de Seguridad y de los mecanismos necesarios para la medir y conocer cómo afectan a la seguridad de la información de la organización las acciones de mejora que se realicen. Estos datos permitirán tomar decisiones al respecto y realizar los ajustes necesarios para el logro de los objetivos.

Para determinar el grado de cumplimiento y de mejora en el tiempo del SGSI se suele plantear un modelo de medición de los objetivos con los siguientes elementos:

- **Los objetivos estratégicos:** Normalmente están determinados por la dirección basándose en la Política de Seguridad de la organización y no son algo estático sino que deben ir ajustándose cada año en relación a los resultados que se vienen registrando, las nuevas necesidades que la organización va detectando o los cambios legislativos que se vengan produciendo. Estos ajustes se realizan normalmente dentro del proceso de "Revisión del SGSI por la Dirección" que establece la cláusula 7 del estándar ISO 27001.
- **Indicadores del sistema:** Los indicadores darán al Comité de Seguridad la información para valorar si los esfuerzos realizados están o no cumpliendo con los objetivos planteados y analizar los posibles riesgos que pueden poner en peligro el éxito de la implantación del SGSI en la organización. Cada indicador debe tener una meta asociada o valor óptimo que se deben alcanzar. En este sentido, cada organización debe definir su propio criterio respecto a qué aspectos quiere controlar y medir para lograr el cumplimiento de los objetivos. Se podrían tener:
    - **Indicadores del grado de efectividad** de las medidas de seguridad. Su sentido es valorar si los controles y las medidas implantadas están funcionando bien o son necesarios ajustes.
    - **Indicadores de medición del entorno y la hostilidad**. Su misión es detectar cambios en el entorno y contexto que rodea al SGSI para realizar ajustes respecto al análisis de riesgos por aparición de nuevas amenazas o cambios en sus frecuencias de ocurrencia

- **Métricas:** Las métricas de seguridad representan los "resultados obtenidos" y son indicadores del valor de ciertos datos relacionados con los aspectos de seguridad en la organización y referentes al comportamiento de una actividad, proceso o control dentro de un tiempo específico y que son necesarios para poder medir de forma real el nivel de seguridad de una organización.
  Habitualmente se utiliza una medida numérica directa que representa un conjunto de datos en relación a una o más dimensiones. Un ejemplo: "Número de infecciones de virus detenidas semanalmente". En este caso, la medida sería un valor entero y la dimensión sería el tiempo. Desde esta perspectiva, un indicador puede tomar información desde diferentes métricas para lograr generar una imagen exacta de lo que está sucediendo dentro del SGSI.

  Para la definición de las métricas es posible utilizar el estándar ISO/IEC 27004:2009 que determina la forma en que se deben realizar las mediciones sobre el estándar ISO 27001. Según la introducción del estándar: *"El empleo de este estándar permitirá a las organizaciones dar respuesta a los interrogantes de cuán efectivo y eficiente es el SGSI y qué niveles de implementación y madurez han sido alcanzados. Estas mediciones permitirán comparar los logros obtenidos en seguridad de la información sobre períodos de tiempo en áreas de negocio similares de la organización y como parte de continuas mejoras".*

  Para que las métricas de seguridad sean efectivas y útiles, deben cumplir con las siguientes premisas:
  - Deben ser relevantes y alinearse con los objetivos de seguridad de la organización.
  - Deben ser reproducibles y justificables.
  - Deben ser objetivas e imparciales.
  - Deben ser capaces de medir la evolución de la seguridad en la compañía a lo largo del tiempo.
  - Deben poder ser utilizables como datos de entrada de procesos de revisión, mejora y auditorías internas de las fases posteriores o como referencia en el cumplimiento de SLA o acuerdos de nivel de servicio con terceros.
  - Se deben poder automatizar los procesos de obtención de medidas y tratamiento de las mismas.
  - Por último deben concienciar al personal de la importancia del sistema de métricas desde el documento de Política de Seguridad.

Estos tres elementos (objetivos, indicadores y métricas) son el núcleo de las actividades de medición del SGSI y se relacionan del siguiente modo: Cada objetivo estratégico tiene unos requisitos de seguridad con los indicadores asociados que miden el grado de cumplimiento del objetivo. Los indicadores a su vez, se alimentarán de una o varias métricas. Este modelo de mediciones queda representado de manera gráfica en el diagrama siguiente.

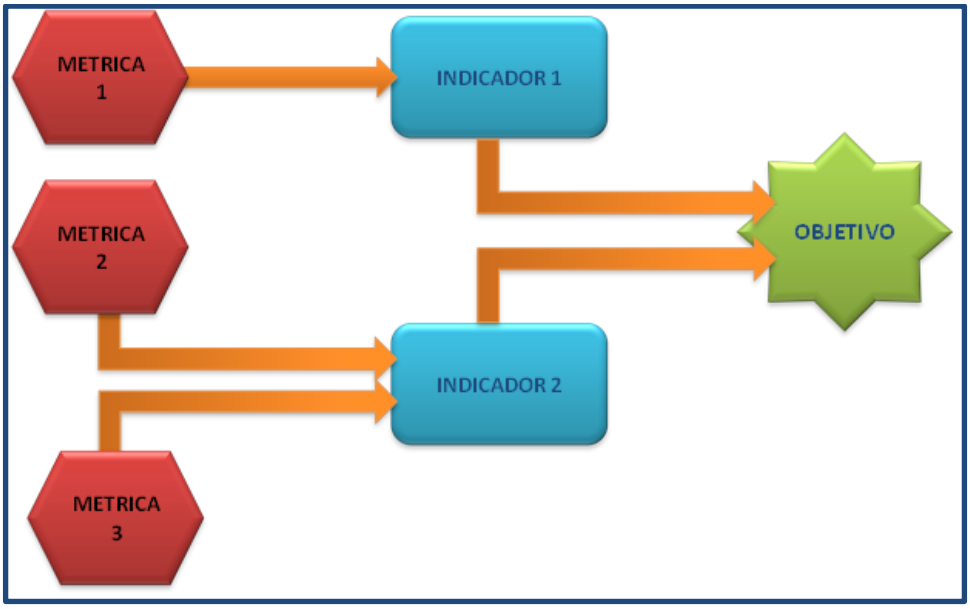



**Ilustración 7: Modelo de medición del SGSI**

Por ejemplo, se podría definir un objetivo con sus indicadores y métricas asociadas del siguiente modo: Se fija el objetivo de **reducir las infecciones por malware en los equipos de la organización** para ello se despliega el control adecuado consistente un proyecto que implanta un antivirus de última generación.

Para comprobar la eficacia se fijan los siguientes indicadores y sus métricas asociadas:

- **Indicador**: Infecciones detectadas y detenidas semanalmente
  - **Métrica**: Número de infecciones detectadas y detenidas mediante firma.
  - **Métrica**: Número de infecciones detectadas y detenidas mediante procedimientos heurísticos.
- **Indicador**: Actualizaciones del archivo de firmas distribuidas semanalmente.
  - **Métrica**: Número de actualizaciones del archivo de firmas.

Una ver implantado el nuevo antivirus y obtenidos los datos de medición (estas tareas se realizarían en las fases 2 y 3 del SGSI) existirían dos opciones:

- **Se alcanza el objetivo**, por tanto la implantación del control ha sido un éxito, los indicadores y las métricas son correctas y el objetivo se puede cumplir. Es posible intentar una mejora de los objetivos en un futuro basándose en un ajuste fino del control (por ejemplo aumentando las actualizaciones del archivo de firmas semanalmente).
- **No se alcanza el objetivo,** pueden existir varias razones para ello:
    - El control no ha sido implantado correctamente.
    - Los indicadores definidos no son los adecuados para estimar la consecución del objetivo.
    - Las métricas no son correctas o no se están obteniendo de manera adecuada.
    - El objetivo planteado es demasiado ambicioso y no es alcanzable.

  En cualquiera de los casos se deben tomar las medidas correctivas adecuadas y realizar el ciclo de medición de nuevo para el estimar el cumplimiento del objetivo.

### 4.2.2 Definir la política de seguridad de SGSI

**El propósito de la Política de Seguridad del SGSI es definir el objetivo, dirección, principios y reglas básicas para la gestión de seguridad de la información en la organización.** No debe ser confundida con la política de seguridad de la información de la organización, sin embargo ambas políticas se suelen fundir en una única política por lo que a partir de ahora se denominará simplemente como Política de Seguridad.

Utilizando la definición del documento RFC 2196 del IETF: ***"Una Política de Seguridad es un documento formal de reglas para todos los usuarios que tienen acceso a los recursos y tecnologías de información de la organización".*** Por tanto **l**a política de seguridad debe comprender todas las reglas de seguridad que se siguen una organización en cuanto a la correcta utilización de los sistemas de información. Por lo tanto debe ser definida por la administración de la organización con ayuda de los expertos en seguridad ya que afecta a todos los usuarios del sistema.

La política de seguridad de la organización es fundamental ya que será la que establezca las bases de las acciones a realizar, mostrará el compromiso de la dirección con el SGSI y servirá para coordinar responsabilidades y tareas. No es una descripción técnica de mecanismos de seguridad, ni una expresión legal que implique sanciones a conductas de los usuarios, sino más bien una descripción de lo que se desea proteger y las razones para ello.

La definición de la **política de seguridad** se suele definir con el objetivo de cubrir las siguientes cuatro necesidades:

- **Identificar las necesidades de seguridad básicas de la compañía** así como sus posibles consecuencias en caso de no cumplirse dichas necesidades.

- **Proporcionar una perspectiva general de las reglas y los procedimientos** que deben implementarse para afrontar los riesgos identificados en los diferentes departamentos de la organización.
- **Controlar y detectar las posibles vulnerabilidades** del sistema de información, y mantenerse informado acerca de las posibles fallas en las aplicaciones y sistemas.
- **Definir funciones y responsabilidades** del personal implicado en el SGSI.
- **Definir Marco jurídico** aplicable al SGSI.
- **Formalizar el apoyo por parte de la Dirección** a la implantación del SGSI.

La política de seguridad es la cúspide del marco normativo relativo de la organización relativo a la seguridad de la información y debe estar perfectamente estructurado para soportar la implantación y el mantenimiento del sistema de gestión requerido por el SGSI (concretamente por ISO 27001). Este marco normativo incluirá los siguientes documentos:

- **Política**: Es la base de la seguridad al constituir la redacción de los requisitos y los objetivos generales en materia de seguridad que quiere llevar a cabo la organización.
- **Procedimientos:** Desarrollan los objetivos marcados en la Políticas. En ellos aparecerán detalles técnicos y se concreta en primera instancia cómo cumplir los requisitos y conseguir los objetivos expuestos en las Políticas.
- **Instrucciones:** Constituyen el desarrollo de los Procedimientos. En ellos se llega hasta el nivel necesario para describir los comandos y acciones técnicas que se deben realizar para el cumplimiento de los requisitos expuestos en los Procedimientos.
- **Registros:** Evidencian la efectiva implantación y el cumplimiento de los requisitos. En este punto es importante contar con una serie de indicadores o métricas de seguridad que permitan evaluar la consecución de los objetivos de seguridad establecidos.

**Ilustración 8: Jerarquía del marco normativo de la organización**

(Fuente: http://www.inteco.es/Formacion/SGSI/Conceptos_Basicos/Normativa_SGSI)

### 4.2.3 Establecer funciones y responsabilidades

Se deben definir al menos los siguientes perfiles en la organización sobre los que recaerán las siguientes funciones:

- **Dirección de la seguridad:** Se asignará un responsable de seguridad, que coordine las tareas y esfuerzos en materia de seguridad. Será el que actúe como centralizador de todos los aspectos de seguridad de la organización y cuyas responsabilidades cubran todas las funciones de seguridad. Además en la mayoría de las organizaciones será necesario designar un comité de seguridad que trate y busque soluciones a los problemas de seguridad, resuelva los asuntos interdisciplinarios y que apruebe directrices y normas.
- **Ejecución de procesos y controles:** Perfiles encargados de la ejecución e implantación de procesos y controles que busquen con el objetivo de minimizar los riesgos para la organización.
- **Revisión del SGSI:** Perfiles encargados de realizar las auditorías y revisiones periódicas del SGSI de manera independiente y veraz.
- **Formación y concienciación:** Se deberán planificar y asignar las responsabilidades en los diferentes grados de formación y concienciación de los miembros de la organización en lo tocante a la seguridad de la información.

### 4.2.4 Realizar un proceso Análisis de Riesgos

El proceso Análisis de Riesgos es la piedra angular de todo SGSI. Esta actividad permite obtener información sobre dónde residen las posibles o actuales amenazas que afectan o pueden afectar a la seguridad de los activos de información de la organización y que se deben afrontar para alcanzar el nivel de seguridad deseado.

La valoración del riesgo debe identificar las amenazas que pueden comprometer los activos, su vulnerabilidad e impacto en la organización. El análisis de riesgos debe ser proporcional a la naturaleza y valoración de los activos y de los riesgos a los que los activos están expuestos.

Según ISO 27001:2005 todo proceso de Análisis de Riesgos de seguridad de la información permitirá a la organización:

- Definir formalmente los requisitos de Seguridad de la Información en función de sus necesidades, y con ello dimensionar adecuadamente la inversión y la estructura necesaria para soportar la Seguridad de la Información.
- Definir un Programa o Plan Director de Seguridad de la Información formal basado en estándares internacionales.

- Establecer un Sistema de Gestión de Seguridad de la Información (SGSI) conforme al estándar ISO/IEC 27001:2005, con el objetivo de hacer sostenibles en el tiempo todas las iniciativas en materia de Seguridad de la Información.
- En menor medida certificar el SGSI desarrollado para demostrar ante la propia organización y ante cualquier tercero interesado el compromiso y la dedicación a la Seguridad de la Información por parte de la organización.

Es recomendable desarrollar una metodología de análisis de riesgos que conjugue la compatibilidad con las metodologías estándar existentes en la actualidad con las necesidades específicas de la organización en la materia.

En el apartado ANÁLISIS Y GESTIÓN DE RIESGOS se describirá de manera más detallada el proceso del Análisis de Riesgos y las principales metodologías empleadas actualmente y aquellas más adaptadas al mercado español.

### 4.2.5 Gestión del riesgo

Implica clasificar los riesgos a la seguridad mediante obtenidos el **Análisis de Riesgos** en aceptables y no aceptables. Lógicamente, la Gestión del Riesgo debe enfocarse hacia los riesgos que la organización no está dispuesta a aceptar, y se debe clarificar el tratamiento que se va a emplear hasta alcanzar un nivel de riesgo aceptable

El tratamiento más común del riesgo será tratarlo mediante la utilización de los controles o salvaguardas de seguridad adecuados como se expuso anteriormente. Los controles serán los necesarios para prevenir, neutralizar o mitigar la probabilidad de que ocurran incidentes o bien reducir el impacto que tendría en caso de que ocurrieran, además deben ser aplicables a la organización por los criterios que se considere oportuno como características del negocio, tipo de activos de información de los que se disponga, presupuesto de seguridad de la organización...etc.

Los objetivos para la selección de los controles serán los siguientes:

1. **Cumplir con los objetivos estratégicos definidos en el alcance y la política de seguridad** de la organización descritos en los puntos anteriores. Para ello se debe elegir una estrategia de alto nivel para mitigar el impacto y el riesgo y que servirá de base para la selección de los controles del punto siguiente.
2. **Determinar los controles o salvaguardas apropiadas y el grado de profundidad necesario para cubrir los objetivos estratégicos marcados:**
   Los controles seleccionados se recogerán en la **Declaración de Aplicabilidad** y se escogerán entre los expuestos en el ANEXO VI: INVENTARIO DE CONTROLES/SALVAGUARDAS y que pertenecen al Anexo A de la Norma UNE/ISO-IEC 27001 (o UNE/ISO-IEC27002:2005).

En la Declaración de Aplicabilidad se recogerá para cada control del Anexo A de la Norma UNE/ISO-IEC 27001 (punto 4.2.1 j) (o UNE/ISO-IEC27002:2005) si es aplicable o no para la organización (y por tanto será implantado o no) y la justificación razonada para esa decisión. También debe realizarse una breve descripción de cada uno de ellos y el estado en que se encuentran en la actualidad.

3. **Determinar las métricas de efectividad de los controles,** es decir decidir cómo se medirá la eficacia de los controles que se implantarán (por ejemplo en un caso de un antivirus el número de virus detectados frente al número de virus eliminados). Los resultados de las métricas corresponden a los registros del marco normativo descrito en el apartado **Definir la política de seguridad de SGSI.**


**Ilustración 9: Registros de los procesos ISO 27001 y 27002**

(Fuente: http://seguridad-de-la-informacion.blogspot.com.es/2008/06/ms-informacin-sobre-iso-270052008.html)

4. **Aprobación del Riesgo Residual**. La Dirección debe aprobar formalmente el riesgo residual subyacente que ha quedado sin cubrir tras la selección de los controles. (Ver ISO 27001 (punto 4.2.1 h). Mediante una estimación del nivel de riesgo residual existente que tras la implantación de los controles se deberá situar hasta un nivel aceptable por la organización, por lo para ello adicionalmente se deberán determinar los criterios de aceptación del riesgo de la organización (presupuestarios, tecnológicos, de tiempo, organizativos…etc.)

En el apartado ANÁLISIS Y GESTIÓN DE RIESGOS se describirá de manera más detallada el proceso de Gestión de Riesgos y las principales metodologías empleadas actualmente y aquellas más adaptadas al mercado español.

### 4.2.6 Establecer el plan de seguridad y tratamiento de riesgos

Debido a que serán numerosas las actuaciones que se pretenderá realizar, debe establecerse un plan con los plazos, los recursos y las prioridades a la hora de ejecutarlas.

La planificación de los proyectos requerirá considerar diferentes aspectos:

- **Definición de fechas de inicio, finalización e hitos destacados para cada proyecto**. Esta definición permitirá que todos los participantes tengan claros sus objetivos, que el cumplimiento de estos objetivos sea medible y que las desviaciones sobre la planificación se detecten a tiempo y puedan corregirse.
- **Coordinar las actividades de los distintos proyectos que lo requieren, estableciendo funciones y responsabilidades claras** y coordinando los calendarios de los distintos proyectos involucrados.
- **Realizar un seguimiento continuo** de la evolución de los diferentes proyectos a nivel presupuestario, temporal, de calidad, etc.

### 4.2.7 Obtener la aprobación de la Dirección de la Organización

Como punto final, toda la planificación resultante de esta fase debe presentarse a la Dirección de la organización quien deberá dar su aprobación para el arranque de los procesos de implantación.

Es vital lograr en este punto que la Dirección de la Organización comprenda los objetivos a conseguir con el SGSI y conseguir su implicación y compromiso con el proyecto, ya de que de otro modo el proceso fracasaría.

## 4.3 FASE 2: HACER - Implantar del Plan de Seguridad y Tratamiento de Riesgos

En esta fase se implanta el plan de tratamiento de los riesgos detectados en la fase anterior.

Es necesario notar que los procesos de implantación de los controles o salvaguardas suelen ser procesos costosos en recursos ya sea tiempo y/o presupuesto, por lo que suelen agruparse en proyectos priorizados en actuaciones a corto, medio y largo plazo valorando diferentes criterios como:

- La criticidad de los activos a proteger.
- El ratio de efectividad/coste de los controles en la mitigación del grado de riesgo.
- El presupuesto en seguridad de la organización.
- La complejidad de la implantación de los controles.
- Etc.

### 4.3.1 Implantar los controles o salvaguardas

En este punto se realizará la implantación de los controles o medidas necesarios para minimizar o anular el riesgo de materialización de una posible amenaza en forma de incidente de seguridad en los sistemas y que sean aplicables según el **Documento de Aplicabilidad** definido en el apartado anterior según el Plan de Seguridad determinado anteriormente.

Este punto suele constituir la parte central y más costosa de todo SGSI debido al elevado número de controles a implantar y al impacto que muchos de ellos suponen para los procesos y los sistemas, por lo tanto para alcanzar el éxito será necesario dedicar recursos suficientes a la gestión de los diferentes proyectos, para garantizar su coordinación y la calidad del resultado final.

### 4.3.2 Implantar las políticas y procedimientos del SGSI

En esta fase debe llevarse a efecto la implantación del marco normativo de seguridad de la organización definido en la fase anterior.
Los principales documentos a generar son:

- **Política de seguridad.** Con las líneas generales que la organización pretende seguir en cuanto a seguridad de la información.
- **Procedimientos e instrucciones**. Con la descripción de las tareas a realizar para la ejecución de los controles que lo necesiten o de las tareas de administración del SGSI.
- **Registros**. Son las evidencias de que se han realizado las tareas definidas para el SGSI. Son muy importantes de cara a poder medir la eficacia de las medidas implantadas así como para justificar las labores realizadas frente a las auditorías del sistema (tanto internas como externas).

### 4.3.3 Formación y concienciación

Dentro de esta fase es muy importante realizar los procesos de **concienciación y formación** del personal de la organización de cara a que conozcan los objetivos estratégicos de seguridad así como los controles que han sido implantados y cómo les afectan en el desempeño de sus labores en la organización.

### 4.3.4 Implantar las métricas

El seguimiento y comprobación del grado de avance de la implantación de los controles debe ser controlado en todo momento mediante las métricas e indicadores establecidos en la fase 1.

En esta fase ya se dispone de un conjunto de medidas de seguridad (y de un conjunto de líneas futuras de trabajo) que es necesario implantar y que permitirán obtener los datos necesarios para alcanzar los objetivos marcados y por lo tanto el nivel de riesgo considerado tolerable por la Dirección

## 4.4 FASE 3: VERIFICAR - Evaluación de los resultados

Una vez puesto en marcha el plan de seguridad, se debe revisar periódicamente de manera que se detecten posibles desviaciones. Los procesos de monitorización, las auditorías y las revisiones serán la clave para detectar incidencias e identificar fallos de seguridad de manera rápida e inequívoca, por ejemplo pueden haberse producido retrasos en las acciones a tomar o bien haber surgido problemas que no fueron previstos y que hay que solucionar para continuar con el plan.

Si se detectan **no conformidades** o **incumplimientos de los requisitos** del SGSI, deben tomarse las acciones oportunas para corregirlas (en la fase siguiente).

Son dos los objetivos que se persiguen en la etapa de Supervisión y Revisión, desarrollada en el punto 4.2.3 de la ISO 27001:

- **Garantizar la eficiencia del SGSI.** Acometeremos este aspecto mediante revisiones de la documentación y los procesos del SGSI. Aprovecharemos también para corregir el Análisis de Riesgos, e introducir las modificaciones necesarias, tanto en los niveles de riesgo aceptables como en los controles de seguridad implantados. Las Auditorías Internas son elementos imprescindibles para llevar a cabo esta labor.
- **Asegurar la adaptación del SGSI a los cambios**. Toda revisión debe contemplar los cambios que hayan podido producirse en la empresa y su entorno. Estos cambios pueden ser organizativos, de los procesos de negocio, de los activos e, incluso, de las amenazas y vulnerabilidades existentes.

Los procesos de evaluación de resultados se detallan a continuación.

### 4.4.1 Monitorización de las métricas

Partiendo de las métricas definidas en la fase 1 e implantadas en las fase 2 se ejecutarán los procesos de monitorización asociados que permitan obtener los resultados.

Las métricas definidas deben ser poderosas herramientas de comprobación de la eficacia y conveniencia de los controles implantados y determinar si el SGSI funciona de la forma esperada. Los procesos de monitorización serán la clave para detectar incidencias e identificar fallos de seguridad de manera rápida e inequívoca.

### 4.4.2 Realizar auditorías internas del SGSI

Otra de las comprobaciones que se realizan dentro del SGSI es la auditoría interna. Tiene por objeto revisar la eficacia de los controles frente a los posibles incidentes de seguridad que pudieran haber afectado a la organización y por lo tanto ofrecen los resultados esperados en el cumplimiento de los objetivos estratégicos de seguridad de la organización.

Adicionalmente de la eficacia, mediante la auditoría se debe determinar si los controles:

- Están conformes con los requisitos de seguridad identificados.
- Están implementados y mantenidos de manera efectiva.
- Están conformes con los requisitos de la Norma UNE/ISO-IEC 27001.
- Están conformes con la legislación y regulaciones aplicables.
- Existe posibilidad de mejora en su gestión o implementación.
- Están monitorizados correctamente y las métricas son las adecuadas.

### 4.4.3 Revisiones del SGSI por parte de la Dirección

La Dirección de la organización revisará anualmente el estado del SGSI para asegurar su eficacia, incluyendo la política y los objetivos de seguridad, así como las oportunidades de mejora dado que tanto el análisis de riesgos como el desarrollo de un SGSI o de un Plan de Seguridad son iniciativas costosas y que requieren largos periodos de ejecución.

La finalidad es que la dirección se implique de manera activa validando que el SGSI continúa siendo adecuado, eficiente y el nivel de mejora y su evolución es correcto mediante el análisis de la siguiente información:

- Grado de consecución de los objetivos, en relación con los requisitos de seguridad planteados sobre los objetivos estratégicos de seguridad.
- Información actualizada sobre la ejecución de los diferentes proyectos de seguridad, a nivel presupuestario y a nivel de tiempos de ejecución.
- Comparativa del nivel de seguridad de la organización con el nivel de otras organizaciones similares, ya sea dentro o fuera del sector o teniendo en cuenta criterios de volumen, geográficos, etc., mediante la utilización de comparativas y estudios realizados por entidades independientes.

Las revisiones del SGSI por parte de la dirección tendrán las siguientes aplicaciones:

- Gobierno Corporativo.
- Cumplimiento de regulaciones y/o requisitos legales.
- Operaciones o gestión organizacional.
- Certificación de un SGSI.
- Clientes, partners, socios de negocio, etc.
- Mejoras en la implementación y/o eficiencia del SGSI.
- Mejora de procesos.

Las principales tareas a considerar para realizar la medición de los resultados del análisis de riesgos son:

- Definir los objetivos de las mediciones.

- Identificar un conjunto reducido de indicadores relevantes que permita dar información precisa sobre los diferentes aspectos a medir.
- Establecer los mecanismos tecnológicos y operativos que permitan realizar el cálculo de los indicadores de forma rápida y precisa.

Existen muchas formas en que la alta dirección puede revisar el SGSI como, por ejemplo, recibir y revisar un informe generado por el representante de la dirección u otro personal, la comunicación electrónica como parte de reuniones regulares de la dirección en donde también se discutan aspectos tales como objetivos estratégicos…etc.

## 4.5 FASE 4: ACTUAR - Realizar acciones adecuadas.

La implantación del SGSI debe ser un proceso dinámico, de manera primordial la misión del SGSI es situar la seguridad de la información al mismo nivel que cualquier otro objetivo de negocio, y como tal, debe ser optimizado continuamente. Esta etapa corresponde al Capítulo 8 de la ISO 270001.

### 4.5.1 Comprobar la eficacia de las mejoras

Comprobar que la incorporación de controles ha resultado en una mejora de la seguridad de la organización. Este paso es más evidente en caso de sucesivas iteraciones del ciclo de mejora continua en el cual se puede observar si los cambios implantados se traducen en una mejoría del estado de la seguridad en la organización.

Las conclusiones de la comprobación de la eficacia permitirán tener un punto de partida para la realización de las acciones apropiadas del punto siguiente.

### 4.5.2 Realizar las acciones apropiadas

Si se detectan no conformidades en el SGSI, deben tomarse las acciones correctivas oportunas para su solución. "**No conformidad" y "acciones correctivas"** son dos conceptos directamente relacionados con la mejora continua y son desarrollados plenamente por la norma ISO

Una no conformidad es el incumplimiento de un requisito, que en el caso que nos ocupa puede ser un requisito de la Norma o estándar de seguridad, una norma interna de la organización, un requisito contractual o legal, etc.

Posteriormente se deben adoptar las acciones o medidas correctivas correspondientes. Además en esta fase es posible identificar las acciones preventivas y las posibilidades de mejora fruto de las revisiones efectuadas, y mejorar así la efectividad del SGSI.

- **Acciones correctivas:** Destinadas a eliminar la causa de una no conformidad detectada u otra situación no deseable.

- **Acciones preventivas:** Destinadas a eliminar la causa de una no conformidad potencial u otra situación potencial no deseable. Es decir la acción preventiva está destinada a evitar que se pudiera llegar a producir una no conformidad.
- **Acciones de mejora**: Destinadas a mejorar la efectividad de los controles existentes.

Las acciones comprenderán por ejemplo, la selección de nuevos controles, la modificación de los existentes o la eliminación de los obsoletos.

Resulta bastante frecuente que llegada esta fase sea necesario rectificar el alcance inicial del SGSI y adecuarlo para cubrir de manera más eficiente las necesidades detectadas, por lo tanto debe comenzar un ciclo nuevo del proceso PDCA.

### 4.5.3 Comunicar resultados

Se deben comunicar los resultados a todos los implicados en SGSI y especialmente hacer partícipe a la dirección de la organización de modo que pueda tener una visión general:

- Del estado de la seguridad de la información en la organización.
- De la evolución en el tiempo de la seguridad en la organización.
- De las acciones y proyectos realizados y su impacto en la evolución frente al coste.

## 4.6 REQUISITOS DE DOCUMENTACIÓN

Toda la documentación y registros generada por el SGSI debe ser aprobada por la Dirección antes de proceder a su distribución formal en la organización. La Norma ISO/IEC 27001 exige, además, cierto grado de protección y un estricto control y gestión de la documentación, basado en versiones, actualizaciones periódicas y sus correspondientes aprobaciones por parte de la Dirección de la empresa.

Los requisitos de la documentación vienen descritos en el punto 4.3 de ISO/IEC 27001:2005.
Los documentos que la Norma marca como obligatorios en todo SGSI son los siguientes:

- **Documento de alcance del SGSI.**
- **Política del SGSI.**
- **Metodología empleada para evaluar el riesgo**.
- **Informe del Análisis de Riesgos.**
- **Plan de Tratamiento del Riesgo.**
- **Autorización y compromiso por escrito de la Dirección** con el SGSI.
- **Declaración de Aplicabilidad** de los controles.
- **Procedimientos documentados**, que aseguren la efectiva planificación, operación y control de los procesos de seguridad del SGSI.

- **Registros que permitan demostrar que el SGSI está operativo en todo momento**. Los registros comprenden desde normativas hasta informes de auditoría. Para más información consultar los puntos 4.2.3, 4.3.1 y 4.3.3 de ISO/IEC 27001.2005.

Los procesos de control de la documentación deben asegurar la edición, aprobación, distribución, revisión y eliminación de los documentos del SGSI. Esto es, la gestión total del ciclo de vida de la documentación del SGSI, y por supuesto también debe garantizar la protección de la Autenticidad, Integridad y Disponibilidad de los documentos y registros asociados al SGSI.

# 5. ANÁLISIS Y GESTIÓN DE RIESGOS

## 5.1 INTRODUCCIÓN AL PROCESO DE ANÁLISIS Y GESTIÓN DE RIESGOS

Como se comentó en los apartados anteriores la piedra angular de todo SGSI es la realización del pertinente análisis de riesgos (o AARR) asociado a los activos de información de la organización. Incluso algunas de las acciones realizadas son compartidas por el SGSI y el AARR como se verá posteriormente.

Para ello, la organización debe construir lo que será su "modelo de seguridad": Partiendo de una representación de todos sus activos y sus dependencias jerárquicas, así como el mapa de riesgos y amenazas (es decir todas aquellas circunstancias que pudieran ocurrir y que tuvieran un impacto para la organización), se realiza la estimación de impactos (probabilidad de que se materialice la amenaza) y se calcula el riesgo al que está sometida la organización.

De un proceso de Análisis de Riesgos se obtendrá el:

- **Inventario valorado de activos.** Con la descripción de los activos de información de la organización, sus relaciones jerárquicas y su grado de valor para la misma.

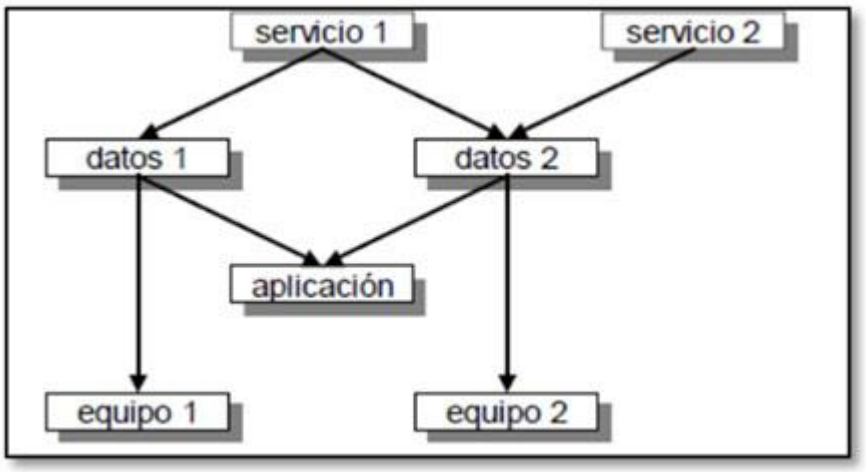



**Ilustración 10: Árbol de activos de la organización**

(Fuente: http://www.securityartwork.es/2012/04/26/analisis-de-riesgos-con-magerit-en-el-ens-ii/)

- **Evaluación del análisis de riesgos.** El escenario de riesgos debe cubrir los sistemas afectados por el SGSI junto con los valores de riesgo de cada uno de los activos. Gracias a la evaluación del análisis de riesgos se podrán justificar lo siguiente:
  - Los controles pertinentes y aplicables a la organización y justificar aquellos que no apliquen a los activos de información de la organización.
  - El grado de profundidad de implantación requerido en los controles aplicables.
  - La necesidad de aplicar un tratamiento adecuado para los riesgos identificados, implantado las salvaguardas necesarias para reducir el riesgo residual aceptable en la organización.

El diagnóstico obtenido del AARR es válido sólo para ese momento puntual en el tiempo y por tanto no es algo estático sino cambia a lo largo del tiempo por diversas razones:

- Nuevos activos o desaparición de los antiguos
- Nuevas amenazas
- Modificación en la posibilidad de ocurrencia de las amenazas.
- Nuevas relaciones o dependencias entre activos…etc.

Por tanto, de manera periódica la organización debe replantearse su diagnóstico y cuestionarse si el modelo o escenario de su seguridad ha cambiado y debe replantearse sus prioridades y objetivos.
La mejora continua afecta también al riesgo ya que si los niveles más altos se han solucionado, lo lógico es plantearse para el siguiente año atacar los siguientes.

## 5.2 OBJETIVOS Y DESTINATARIOS DEL PROCESO DE ANÁLISIS Y GESTIÓN DE RIESGOS

De manera general y como se ha comentado anteriormente el objetivo de un proceso de Análisis y Gestión de Riesgos será el de identificar, cuantificar y evaluar las amenazas que pueden poner en riesgo a los activos de información de la organización. Una vez identificado el nivel de riesgo existente, se deben identificar e implantar las salvaguardas, controles o medidas de protección que son necesarias para reducir el riesgo residual a un nivel aceptable en la organización.

Teniendo en cuenta lo expuesto en el punto anterior, el Análisis de Riesgos en la organización tiene como objetivos:

- **Reducir el riesgo en la seguridad de la organización:** Es el objetivo principal del proceso de análisis de riesgos. La implantación de las salvaguardas adecuadas reducirá de manera efectiva la posibilidad de ocurrencia de una situación que afecte a la seguridad de la información de la organización.
- **Facilitar y justificar la toma de decisiones:** Los recursos disponibles en las organizaciones suele ser limitado como para plantear para la implantación de todas las posibles medidas o controles de seguridad recomendadas por ISO 27002 u otros códigos de buenas prácticas. El análisis de riesgos ayudará determinar cuáles son los principales riesgos de Seguridad de la Información que podrían afectar a los activos más valiosos de la organización, determinar cuáles son las medidas que reducen en mayor medida este riesgo y en base ello decidir cuáles medidas o controles se deben priorizar en base a los recursos disponibles y justificar las decisiones tomadas.

- **Optimizar la utilización de recursos en seguridad:** Siguiendo con lo comentado en el punto anterior, no suele ser posible para las organizaciones por razones de coste afrontar la implantación de todas las salvaguardas o medidas de protección contra las posibles amenazas que pueden afectar de forma negativa a los activos. Por ello es necesario definir un proceso que permita identificar aquellos riesgos que deben tenerse en especial consideración frente a aquellos que, debido a su baja probabilidad de ocurrencia, su bajo impacto o su alta dificultad o coste de su mitigación, deban ser asumidos por la organización o puedan ser abordados con posterioridad.
- **Cumplir con las normativas aplicables:** La necesidad de llevar a cabo un análisis de riesgos suele formar parte de los requisitos de cumplimiento de multitud de normas y regulaciones. A nivel legal en España cabe destacar las siguientes:
    - Real Decreto 3/2010, de 8 de enero, establecido en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. (Esquema Nacional de Seguridad).
    - Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
    - Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y sus desarrollos reglamentarios (LOPD)

Algunos de los principales destinatarios de los resultados del proceso de Análisis y Gestión de riesgos son:

- **Los responsables de seguridad de la información**: Les permite obtener y formalizar la información sobre la situación actual y deseable de seguridad, y así definir el plan de acción necesario para cumplir los requisitos de la organización.
- **La Dirección de la organización**: Permite transmitir a la dirección de la organización la necesidad de establecer medidas contra los riesgos que amenazan la consecución de los objetivos fijados, el plan de acción propuesto para alcanzar el nivel de seguridad adecuado y la inversión asociada para tomar las decisiones oportunas y proporcionar la financiación necesaria.
- **Auditores:** Les permite obtener un profundo conocimiento de los riesgos existentes en la organización, que emplean en su función de evaluar el cumplimiento de las políticas y procedimientos establecidos para mitigarlos.

## 5.3 EL PROCESO DE ANÁLISIS Y GESTIÓN DE RIESGOS Y EL SGSI

Como se ha comentado anteriormente el aprovechamiento completo del SGSI y por tanto de la herramienta, es muy recomendable que la organización realice previamente un proceso de Análisis y Gestión de Riesgos de sus Sistemas de Información que permita cuantificar y comparar los requisitos de seguridad de la información que debe cubrir la organización mediante implantación de las salvaguardas o controles adicionales necesarios para el cumplimiento de todos los requisitos de seguridad de la información aplicables.

El proceso de Análisis y Gestión de Riesgos es considerado una pieza fundamental para la Seguridad de la Información por diversos estándares y códigos de buenas prácticas y en concreto por los estándares en los que se basa la herramienta:

- **ISO/IEC 27001:2005** Tecnología de Información – Técnicas de seguridad – Sistemas de Gestión de Seguridad de la Información – Requisitos
- **ISO/IEC 27002:2005** Tecnología de Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información

Algunos otros ejemplos de estándares y códigos de buenas prácticas que prescriben la realización de un proceso de Análisis y Gestión de Riesgos son:

- **Esquema Nacional de Seguridad (ENS: RD 3/10)**
- **ISO/IEC 20000 Tecnología de información:** Gestión del servicio.
- **NIST SP 800-53:** Controles de seguridad recomendados para los sistemas de información federales en EEUU.
- **ITIL**: Information Technology Infrastructure Library
- **COBIT** : Control OBjectives for Information and related Technology
- **BS 25999:2006:** Gestión de continuidad de negocio

El ejercicio de análisis de riesgos no debe entenderse aislado del resto de iniciativas destinadas a conseguir un nivel de seguridad acorde con los requisitos de la organización.
Por ejemplo en caso que la organización establezca un nivel mínimo de seguridad que especifique un conjunto de medidas básicas de seguridad que deben cumplirse en todos los entornos de la organización, el análisis de riesgos puede centrarse en analizar aquellos otros riesgos que necesitan una atención, y por tanto, unas medidas de seguridad especiales o adicionales.

## 5.4 PROCESO DE ANÁLISIS Y GESTIÓN DE RIESGOS

El proceso de análisis y gestión de riesgos de riesgos consiste en una serie de técnicas que determinará los activos de información valiosos para la organización, valorarlos en base a la medida en que el desarrollo normal del negocio se vería afectado por su pérdida y determinar aquellos eventos o amenazas a los que está expuesto que pudieran afectarlos negativamente. El resultado es un mapa de riesgos y una valoración de los activos en base a su nivel o estado de riesgo que determina las posibles pérdidas de la organización.

Por lo tanto la evaluación de riesgos es una herramienta básica para gestionar la seguridad de los SSII que permite identificar, clasificar y valorar los eventos que pueden amenazar la consecución de los objetivos de la organización y consecuentemente establecer las medidas oportunas para reducir el impacto esperable hasta un nivel tolerable para la organización.

El análisis de riesgos además permite cuantificar cuál es el coste de la inseguridad (riesgo) que asume una organización en un momento determinado, y cómo evoluciona este coste en función de las medidas de seguridad que se implementen. De esta forma el análisis de riesgos permite determinar cuándo una determinada medida de seguridad va a suponer una reducción del riesgo menor que su propio coste, y, por tanto, no es aconsejable su implantación desde un punto de vista económico.

El desarrollo del Análisis de Riesgos se podrá realizar mediante cualquiera de las principales metodologías de análisis y gestión de riesgos de uso habitual en los entornos de seguridad de la información o bien mediante cualquier otra metodología desarrollada a medida y basada en las necesidades, cultura y estructura específicas de la organización

Los resultados del proceso de Análisis y Gestión de riesgos deben presentar dos características fundamentales:

- **Objetividad:** Diferentes personas, aplicando el mismo proceso sobre el mismo entorno, deberían obtener resultados idénticos.
- **Valoración:** Todos los riesgos y las medidas de seguridad potencialmente aplicables para mitigarlos quedan priorizadas utilizando una escala que puede ser numérica (en el caso del análisis cuantitativo) o literal (en el caso del análisis cualitativo).

Básicamente todo proceso de análisis y gestión de riesgos consta principalmente de dos fases:

- **Fase de Análisis de Riesgos:**
    - Determinación de activos
    - Determinación de amenazas
    - Estimación de impactos
    - Estimación de vulnerabilidad de las amenazas sobre los activos
    - Cálculo del nivel de riesgo.
- **Fase de Gestión, tratamiento o mitigación de los riesgos** detectados en la Fase 1

- Determinación de los criterios de aceptación del riesgo
- Determinación de las medidas de seguridad necesarias
- Planificación e implantación de las medidas o controles
- Estimación del nivel de riesgo residual y evaluación de los resultados obtenidos

### 5.4.1 Fase de Análisis de Riesgos

Esta fase es el núcleo central de todo AARR, su correcta aplicación condiciona la validez y utilidad de todo el análisis. La identificación y estimación de los activos y de las posibles amenazas que les pueden afectar representa una tarea compleja.

**En el caso de implantación de un SGSI esta fase corresponde al apartado "Realizar un proceso Análisis de Riesgos" del presente documento.**

Los objetivos son los siguientes:

- **Desarrollar un modelo del valor del sistema, identificando y valorando los activos relevantes.** Los activos pueden ser:
  - **Primarios:** Información y procesos y actividades de negocio de la organización.
  - **De soporte**: Hardware, software, redes de comunicaciones, centro de proceso de datos, personal...etc.
- **Desarrollar un mapa de riesgos del sistema, identificando y valorando las amenazas** a la seguridad de la información sobre los activos identificados.
- **Conocer situación actual** de salvaguardas.
- **Evaluar el impacto posible sobre el sistema** en estudio, tanto **el impacto potencial** (sin salvaguardas), como **el impacto residual** (incluyendo el efecto de las salvaguardas implementadas si se trata de un sistema actual, no de un sistema previsto).
- **Evaluar** los distintos valores de riesgo del entorno en estudio:
  - **Riesgo potencial:** Excluyendo todas las salvaguardas.
  - **Riesgo efectivo:** Incluyendo el efecto de las salvaguardas ya implementadas.
  - **Riesgo residual:** Incluyendo el efecto de las salvaguardas a implementar en el entorno previsto.
- **Mostrar al Comité de Dirección las áreas del negocio** cuyos sistemas de información presentan mayor impacto y/o riesgo.

Para realizar lo anterior, las tareas más habituales en esta fase incluyen las siguientes:

- Caracterización de activos de información:
  - Identificación de los activos de los procesos de negocio.
  - Valoración de los activos por su nivel de criticidad para el negocio.
  - Dependencias entre activos y propagación de valor del activo.
- Caracterización de amenazas a los activos de información

- Identificación y valoración de amenazas
- Caracterización de salvaguardas
  - Identificación y valoración de salvaguardas existentes
- Estimación del nivel de riesgo:
  - Estimación del grado de vulnerabilidad de los activos a las amenazas
  - Estimación del impacto de materialización de la amenaza
  - Estimación de probabilidad de materialización de la amenaza
  - Interpretación de los resultados.

La valoración de los activos se elaborará mediante el método que mejor se ajuste a las necesidades de la organización. Un método usual suele ser la utilización de matrices de evaluación del nivel necesario (Alto, Medio, Bajo) de cada uno de los requisitos de los principios básicos de seguridad del activo (Confidencialidad, Integridad, Disponibilidad o CID) y de otros requisitos como el tipo de usuarios, el valor estratégico del activo y su nivel de exposición, como la expuesta a continuación.

| REQUISITO DE SEGURIDAD | NIVEL REQUERIDO POR EL ACTIVO | | |
|---|---|---|---|
| | **Alto** | **Medio** | **Bajo** |
| **Confidencialidad** | Información catalogada como SECRETA | Información catalogada como CONFIDENCIAL | Información catalogada como INTERNA o PUBLICA |
| **Integridad** | Información que precisa de un nivel de integridad de NO REPUDIO | Información que precisa de un nivel de integridad de ALTO | Información que precisa de un nivel de integridad ESTANDAR o MINIMO |
| **Disponibilidad** | Tiempo máximo de indisponibilidad < 24 horas | 24 < Tiempo máximo de indisponibilidad < 48 horas | Tiempo máximo de indisponibilidad > 48 horas |
| **Usuarios del Sistema** | El conjunto de usuarios del sistema está conformado por los miembros del consejo de dirección o clientes clave | El conjunto de usuarios del sistema está conformado por clientes o empleados clave | El conjunto de usuarios del sistema está conformado por empleados de la organización y colaboradores |
| **Valor Estratégico** | El sistema de información será un factor clave del negocio de la organización | El sistema de información apoya un proceso de negocio de la organización | El sistema de información soporta procesos de gestión interna de la organización |
| **Nivel de Exposición** | Sistemas de Información publicados en Internet, de acceso público | Sistemas de Información Accesibles desde el exterior de la organización pero no públicos | Sistemas únicamente accesibles desde las redes internas de la organización |

**Ilustración 11: Matriz de valoración del nivel de seguridad de los activos**

Como ejemplo se presenta el siguiente diagrama representa un árbol jerárquico de los activos valorados conforme al nivel requerido por la organización de los requisitos de los principios básicos de la seguridad del activo (CID). El árbol parte desde el nivel proceso de la organización que depende de otros activos como los sistemas de información, las redes de comunicaciones y en última instancia de las instalaciones de la organización (aunque normalmente no es necesario llegar a un nivel de detalle tan bajo). Como se puede observar los niveles crecientes de requisitos se heredan desde los activos de niveles superiores a los activos de niveles inferiores.

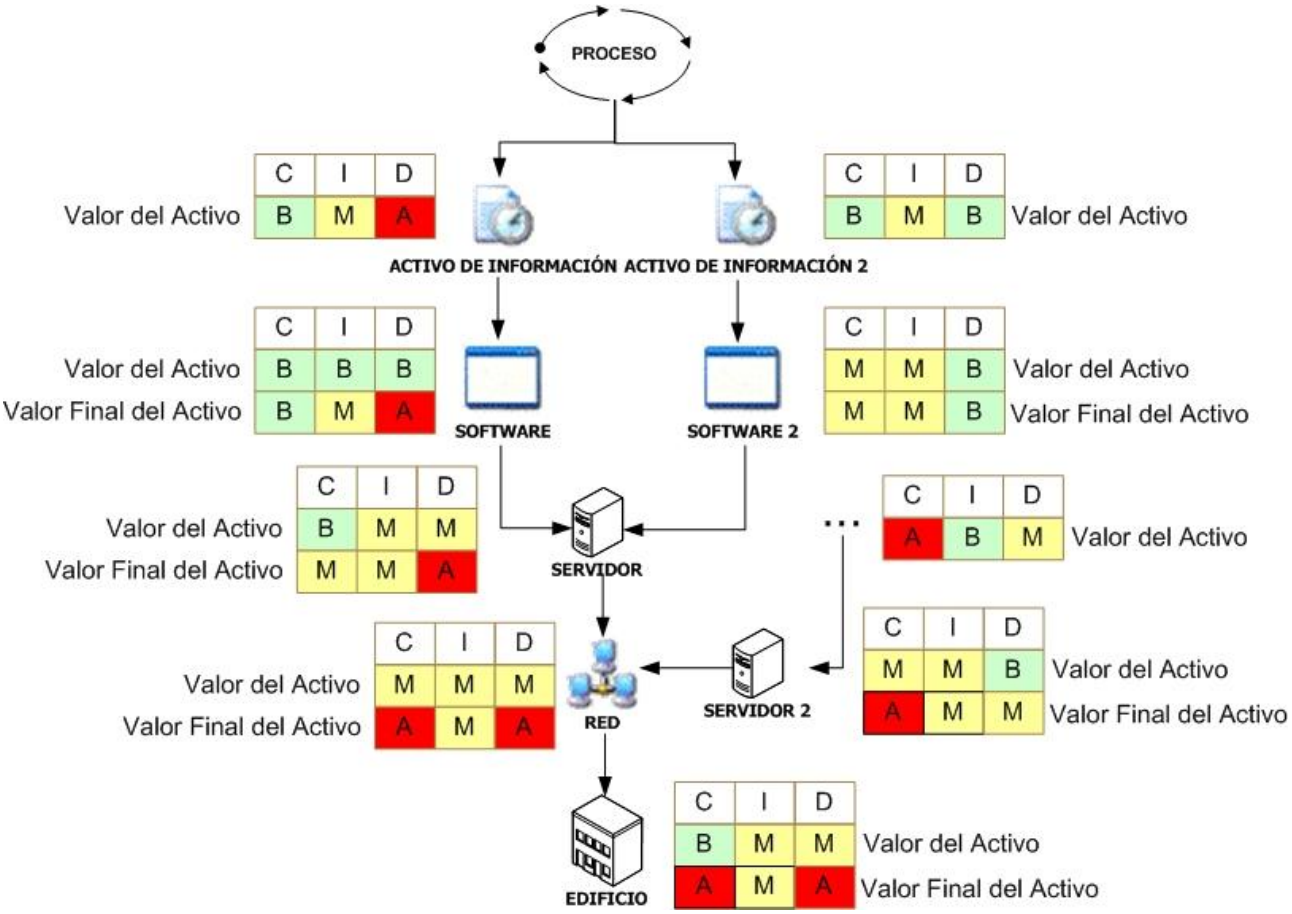



**Ilustración 12: Árbol de activos valorados de la organización**

(Fuente: http://www.miguelangelhernandez.es/)

Para la estimación del nivel de riesgo en cada uno de los activos se suelen utilizar cálculos del riesgo basados en la posibilidad de materialización de las distintas amenazas, en el impacto de las consecuencias que se causa sobre el activo en tal caso y en el valor de la seguridad del activo para la organización, de tal manera que el riesgo repercutido se hereda desde los activos de niveles superiores a los de niveles inferiores.

Una versión simplificada de ese cálculo es mostrada en el gráfico siguiente, donde se pondera la posibilidad de ocurrencia de la amenaza y el impacto de las consecuencias ponderadas respecto al valor del activo para la organización y las necesidades de seguridad de la información respecto a los parámetros de Confidencialidad, Integridad y Disponibilidad obtenidas del paso anterior.

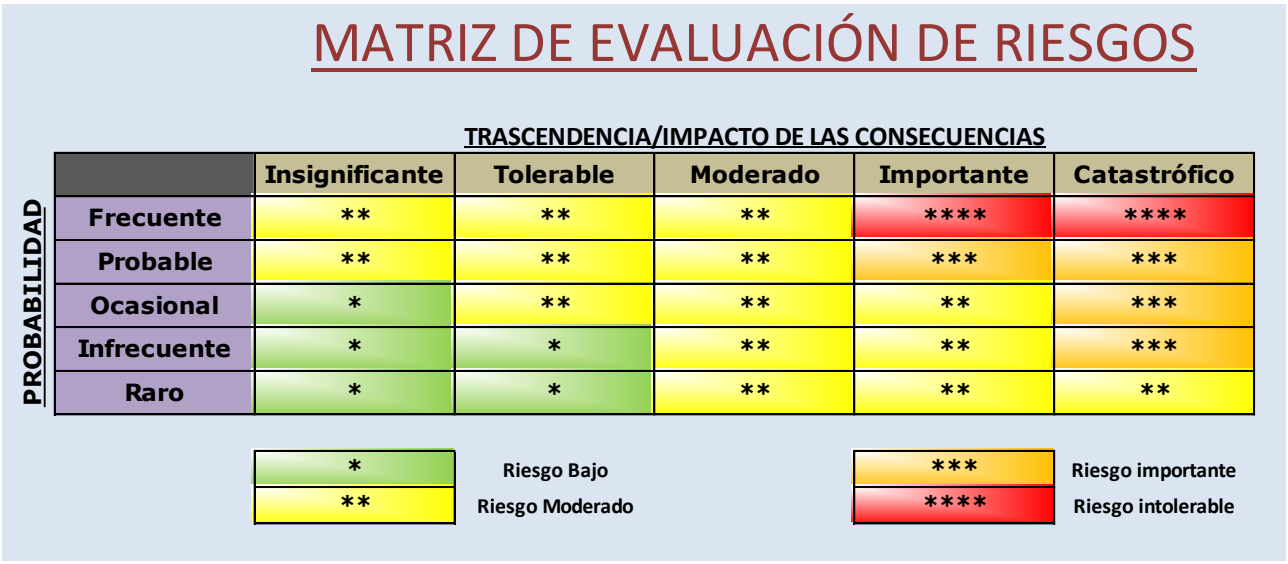



Ilustración 13: Matriz de evaluación de riesgos

Sin embargo dada la complejidad de los cálculos de la estimación del nivel de riesgo es aconsejable utilizar herramientas automatizadas y reconocidas como Pilar para esta tarea.

### 5.4.2 Fase de Gestión de Riesgos

Partiendo del resultado de la fase anterior se decide la estrategia a seguir sobre los riesgos identificados, puede conllevar asumirlos si se consideran aceptables o bien afrontarlos si se consideran inaceptables, para lo cual se llevará a cabo un plan de seguridad que corrija la situación actual.

En el caso de implantación de un SGSI esta fase corresponde a los apartados "Gestión del riesgo", "Establecer el plan de seguridad y tratamiento de riesgos" e "Implantar los controles o salvaguardas" del presente documento.

Los objetivos serán los siguientes:

- **Determinación de los criterios de aceptación del riesgo**: Económicos, técnicos…etc.
- **Elegir una estrategia para mitigar el impacto** y el riesgo.
- **Determinar las salvaguardas oportunas y el grado de profundidad** necesaria para la decisión anterior.
- **Estimación del nivel de riesgo residual.**
- **Diseñar un plan de seguridad** para llevar el impacto y el riesgo a niveles aceptables.
- **Llevar a cabo el plan de seguridad**.

Las tareas más habituales en esta fase incluyen las siguientes:

- Toma de decisiones
    - Calificación de los riesgos
- Plan de seguridad

- Programas de seguridad
- Plan de ejecución

- Ejecución del plan
  - Ejecución de cada programa de seguridad

## 5.5 METODOLOGÍAS Y ESTÁNDARES PARA EL ANÁLISIS DE RIESGOS

Se describen algunas de las metodologías habituales y recomendadas para el desarrollo del análisis de riesgos. Aunque la terminología puede variar entre metodologías, en general todas realizan un análisis basado en el proceso descrito anteriormente.

### 5.5.1 MAGERIT

La metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de IT) fue desarrollada por el Consejo Superior de Administración Electrónica (CSAE) y fue publicada por el Ministerio de Administraciones Públicas (MAP), actualmente es publicada por CCN-CERT.

Se trata de una metodología pública y abierta de uso muy extendido en el ámbito español y uso es obligatorio en proyectos de la Administración Pública Española y está reconocido por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA : European Network and Information Security Agency) junto a otras metodologías europeas e internacionales.

La primera versión se publicó en 1997, y la versión actual es v3.0 de Octubre de 2012 aunque en el presente documento se utilizará la versión 2.0 publicada en 2006. No se tratará MAGERIT V3 por ser demasiado reciente y las novedades están más orientadas a la integración con el estándar ISO 31000/2009 relacionado con principios generales de una gestión de riesgos genérica, no orientada a ningún proceso o sector determinado.

La metodología MAGERIT se puede resumir gráficamente de la siguiente forma:

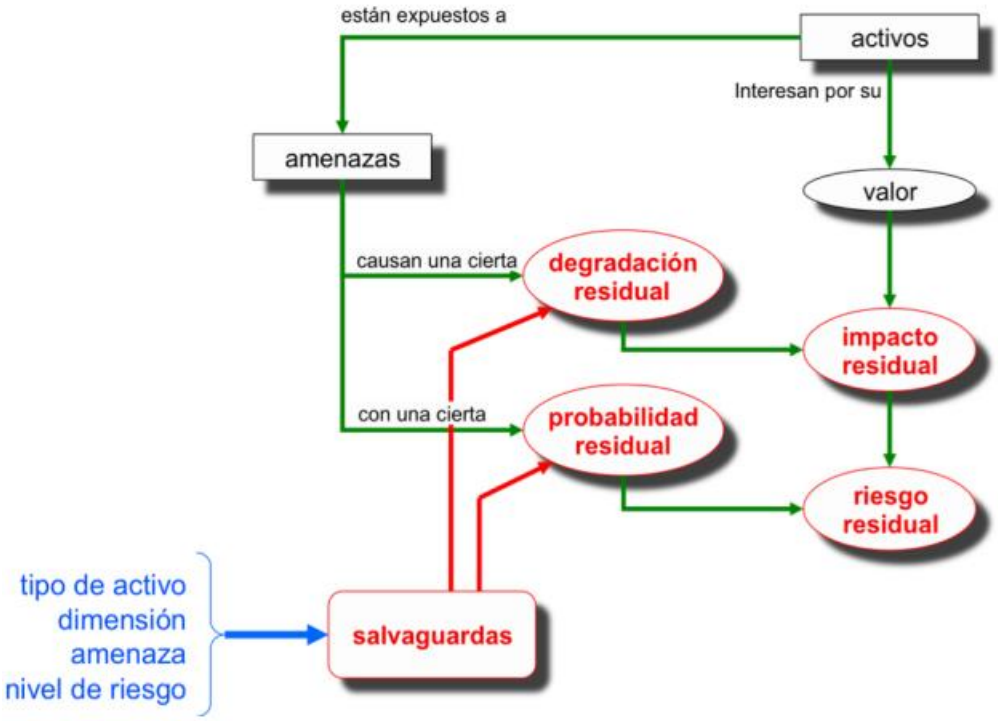



**Ilustración 14: Modelo del proceso de Magerit**

(Fuente: http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=P80029225129365155099 1&langPae=es&detalleLista=PAE_12765296834971 33)

La metodología consta de tres volúmenes:

- **Volumen I** – Método, es el volumen principal en el que se explica detalladamente la metodología.
- **Volumen II** – Catálogo de elementos, complementa el volumen principal proporcionando diversos inventarios de utilidad en la aplicación de la metodología.
  Los inventarios que incluye son:
  - Tipos de activos
  - Dimensiones y criterios de valoración
  - Amenazas
  - Salvaguardas
- **Volumen III** – Guía de técnicas, complementa el volumen principal proporcionando una introducción de algunas de técnicas a utilizar en las distintas fases del análisis de riesgos.
  Las técnicas que recoge son:
  - Técnicas específicas para el análisis de riesgos:
    - Análisis mediante tablas
    - Análisis algorítmico
    - Árboles de ataque

- Técnicas generales
    - Análisis coste-beneficio
    - Diagramas de flujo de datos (DFD)
    - Diagramas de procesos
    - Técnicas gráficas
    - Planificación de proyectos
    - Sesiones de trabajo: entrevistas, reuniones y presentaciones
    - Valoración Delphi.

MAGERIT dispone de una herramienta de soporte oficial: **PILAR** (Proceso Informático-Lógico para el Análisis y la gestión de Riesgos), de uso gratuito para la Administración Pública española y comercial para organizaciones privadas.

La metodología MAGERIT es gratuita y se puede obtener en la siguiente dirección: http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184

### 5.5.2 ISO/IEC 27005

El estándar ISO/IEC 27005 es un estándar de seguridad de la información publicado por las organizaciones ISO e IEC (descritas en el apartado 2.2 del presente documento) y forma parte de la familia ISO/IEC 27000 relativa a seguridad de la información. El título completo de la versión utilizada es **ISO/IEC 27005: Information technology – Security techniques – Information security risk management**.

Se trata, quizás, de una de las normas más estructurales de la serie ya que establece un criterio sobre la gestión del riesgo y proporciona un marco normalizado que nos puede ayudar a definir nuestra propia metodología y que tiene por título ISO/IEC 27005:2008 (Information technology, Security techniques, Information security risk management) y proporciona una base para la gestión del riesgo en un sistema de seguridad de la información.

El propósito del estándar ISO/IEC 27005 es el de proveer un marco de actuación para la gestión del riesgo de la seguridad de la información. Comparte conceptos, modelos, procesos y terminología con los estándares ISO/IEC 27001 e ISO/IEC 27002 y se diseñó con el objetivo de dar soporte en un proceso de mejora de la seguridad de la información a través de la gestión del riesgo. Constituye, por tanto, una ampliación del apartado 4.2.1 de la normativa ISO/IEC 27001, en el que se presenta la gestión de riesgos como la piedra angular de un SGSI, pero sin prever una metodología específica para ello.

Esta norma sustituye a las anteriores normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000. La versión actual es de 2011 (ISO/IEC 27005:2011) en línea con el estándar ISO 31000/2009_sobre principios generales de una gestión de riesgos genérica y no orientada a ningún sector determinado.

ISO/IEC 27005 no proporciona una metodología concreta de Análisis de Riesgos, sino que proporciona un conjunto de directrices para la correcta realización de un Análisis de Riesgos mediante la descripción de un proceso estructurado, riguroso y sistemático de los elementos que debe incluir toda buena metodología de Análisis de Riesgos a través del clausulado de las fases que lo conforman:

- Establecimiento del contexto (Cláusula 7)
- Evaluación del riesgo (Cláusula 8 )
- Tratamiento del riesgo (Cláusula 9)
- Aceptación del riesgo (Cláusula 10)
- Comunicación del riesgo (Cláusula 11)
- Monitorización y revisión del riesgo (Cláusula 12)

Una de las ventajas de ISO/IEC 27005 es que expone un catálogo relativamente amplio de amenazas en su Anexo C.

Este estándar solamente puede obtenerse a través en la página de ISO o los distribuidores autorizados.
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56742

### 5.5.3 NIST SP 800-30

El estándar "**NIST SP 800-30: Guía de Gestión de Riesgos de los Sistemas de Tecnología de la Información"** es una publicación del Instituto Nacional de Normas y Tecnología (NIST por sus siglas en inglés, National Institute of Standards and Technology), fue publicada en 2002, aunque la última revisión se publicó en Octubre de 2012.

NIST es la agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competitividad industrial de Estados Unidos mediante avances en tecnología y normalización de mediciones, creación de normativas y tecnología que mejoren la estabilidad y seguridad económica.

El NIST ha dedicado una serie de publicaciones especiales, la serie SP 800 a la seguridad de la información. Esta serie incluye una metodología para el análisis y gestión de riesgos de seguridad de la información, alineada y complementaria con el resto de documentos del instituto.

En la Fase 1 de Análisis de riesgos NIST SP 800-30 expone 9 pasos principales según está expuesto en el siguiente diagrama:

- Paso 1: Caracterización del sistema (System Characterization)
- Paso 2: Identificación de las amenazas (Threat Identification)
- Paso 3: Identificación de las vulnerabilidades (Vulnerability Identification).
- Paso 4: Análisis de control (Control Analysis)
- Paso 5: Determinación de la probabilidad del riesgo (Likelihood Determination)
- Paso 6: Análisis de impacto (Impact Analysis)
- Paso 7: Determinación del riesgo (Risk Determination)
- Paso 8: Recomendaciones de controles (Control Recommendations)
- Paso 9: Documentación de los resultados (Results Documentation)

Los pasos de la fase 1 se pueden resumir en el siguiente diagrama

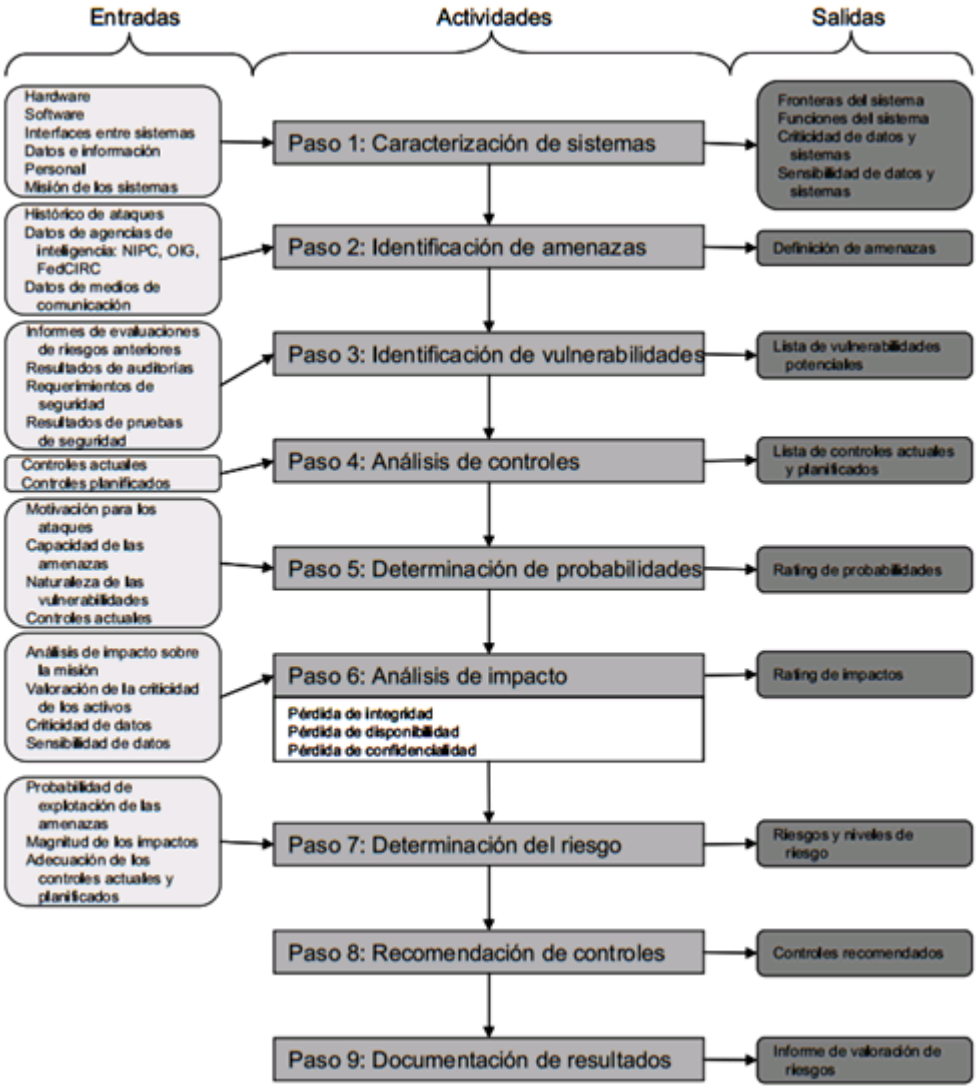



**Ilustración 15: Workflow de la Fase 1 de NIST**

(Fuente: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)

En la Fase 2 de Mitigación del Riesgo se realiza la gestión del riesgo mediante la exposición de las estrategias adecuadas de mitigación del riesgo y la implementación de controles que implica priorizar, evaluar e implementar los controles de reducción del riesgo apropiados y que son determinados en la fase anterior.

Para la fase de implementación de controles los pasos son los siguientes:

- Paso 1: Priorización de las acciones (Prioritize Actions)
- Paso 2: Evaluar las opciones de los controles recomendados (Evaluate Recommended Control Options)
- Paso 3: Realizar análisis coste-beneficio (Conduct Cost-Benefit Analysis).
- Paso 4: Selección de controles (Select Control)
- Paso 5: Asignación de responsabilidades (Assign Responsibility)
- Paso 6: Desarrollar un plan de implantación de las salvaguardas (Develop a Safeguard Implementation Plan)
- Paso 7: Implantar los controles seleccionados (Implement Selected Control(s))

Los pasos de la fase 2 se pueden resumir en el siguiente diagrama

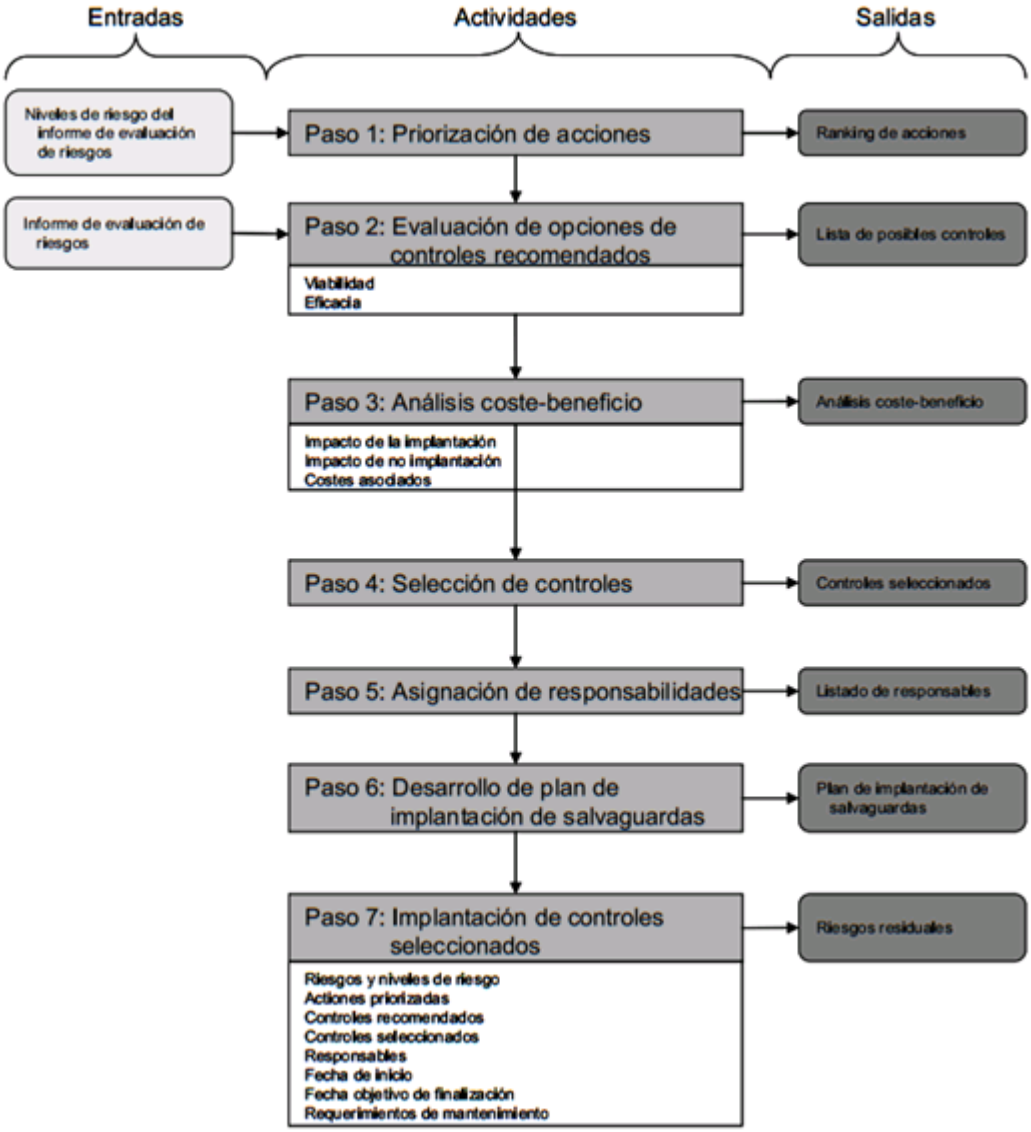



**Ilustración 16: Workflow de la Fase 2 de NIST**

(Fuente: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)

La guía NIST SP 800-30 es gratuita y se puede obtener en la siguiente dirección: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

# 6. DESARROLLO DE LA HERRAMIENTA

## 6.1 MOTIVACIÓN DEL DESARROLLO DE LA HERRAMIENTA

En los apartados anteriores se ha expuesto la situación con respecto las necesidades en la gestión de la seguridad en las diversas organizaciones y las diferentes metodologías y estándares internacionales que pueden ser de ayuda en la mejora de la seguridad de la información en la organización.

Sin embargo la implantación de estos estándares suele ser compleja sin una experiencia previa o sin unas herramientas de ayuda y es precisamente para cubrir este punto donde toma forma el objetivo del proyecto: **Recoger el conocimiento y la experiencia profesional del autor del proyecto relativa a en seguridad en sistemas de información en una herramienta que sea un soporte para el proceso de implantación de SGSIs y que aportaría sustanciales beneficios en los procesos de gestión de la seguridad de la información en las organizaciones.**

Los beneficios aportados por la herramienta serían los siguientes:

- Permitiría una reducción del esfuerzo dedicado a la realización de la gestión de la seguridad, facilitaría una visión global en todo momento del estado de seguridad en la organización y permitiría una revisión de la evolución en el tiempo del nivel de seguridad.
- Ayudará al área de seguridad de la organización en la gestión del estado de madurez e implantación de los controles correspondientes en la organización, de su efectividad así como el seguimiento del objeto mediante la gestión de los proyectos, auditorías, informes, métricas y cuadros de mando correspondientes que faciliten y permitan el seguimiento de la evolución de un proyecto de implantación de un SGSI en la organización.
- Por otra parte también permitirá trasladar a la dirección de la organización la evolución y la justificación del empleo de los recursos en la mejora de la seguridad y a auditores externos la justificación en caso de cumplimiento de normas o procedimientos para certificaciones de terceros.
- Así mismo la herramienta permitiría la centralización de la información relativa al estado de la evolución de la seguridad de la información en la organización ya que tradicionalmente el desarrollo en el tiempo de un proceso de implantación de un SGSI genera gran cantidad de datos e información en distintos formatos (Excel, Word...etc.) que suelen estar dispersos y no controlados. Esta información por su naturaleza confidencial debe estar centralizada, disponible y su acceso controlado únicamente a los responsables de seguridad de la información en la organización.
- Si bien utilización de la herramienta está prevista principalmente en el proceso de implantación de un SGSI, aunque también sería posible utilizarla como simple ayuda a la implantación y seguimiento de controles aislados, si bien esta circunstancia no permite el aprovechamiento completo de la misma dentro de un proceso de mejora continua.

- Así mismo la herramienta podrá recoger y analizar datos de herramientas de terceros relativas a pruebas de cumplimiento de los controles y por último podrá integrarse con los repositorios de autenticación corporativos y permitir una administración centralizada.

Todas estas características quedarían reflejadas en el siguiente diagrama general de la herramienta que se denominará HIS-SGSI (Herramienta de Implantación y Seguimiento de SGSI).

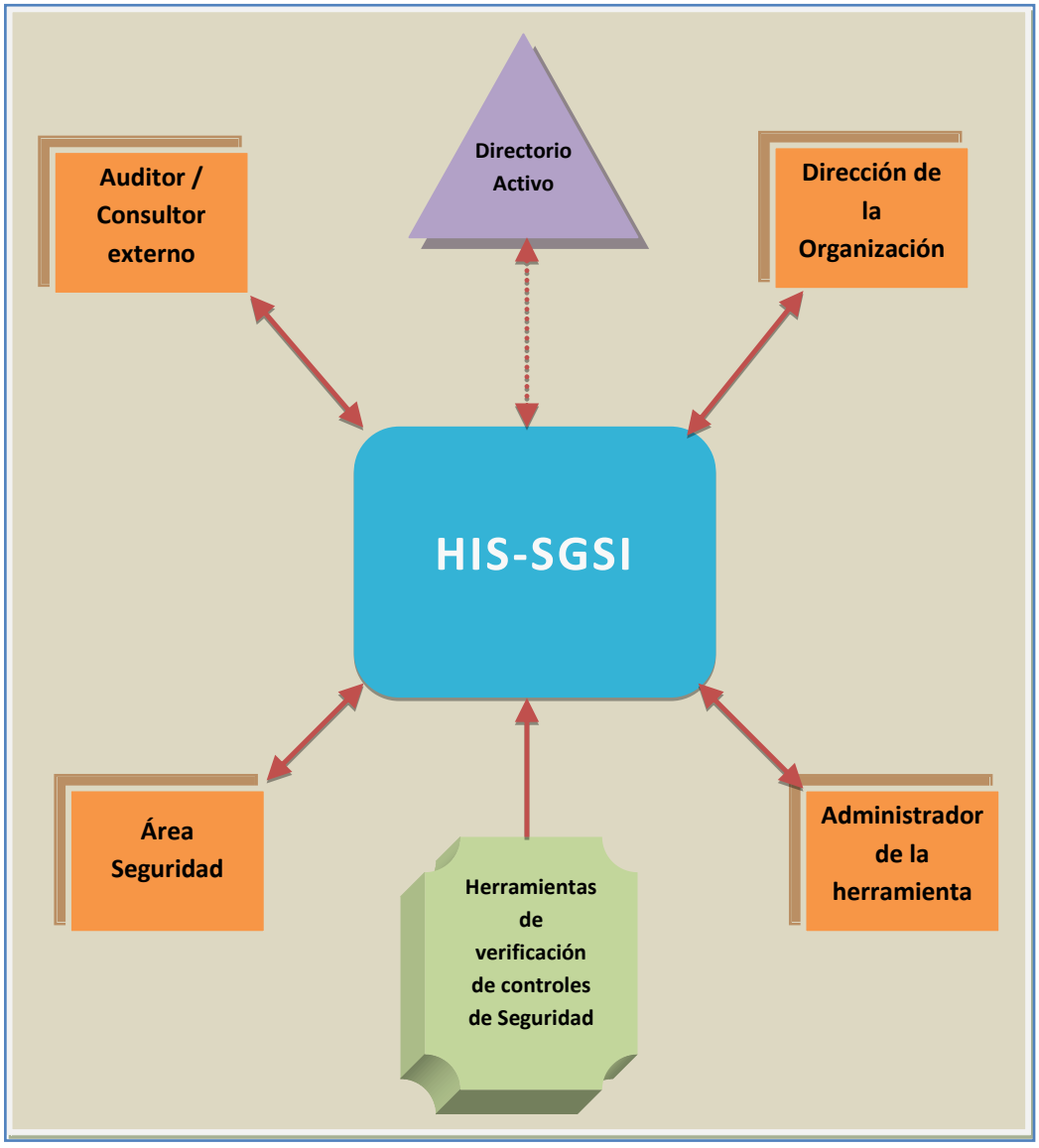



Ilustración 17. Diagrama de contexto del sistema

## 6.2 ESTIMACIÓN DE COSTE Y ESFUERZO DE DESARROLLO DE LA HERRAMIENTA

Este apartado expone la estimación de coste de la herramienta, los recursos y el tiempo empleado en su desarrollo, esta estimación se utilizó inicialmente para el estudio de la viabilidad del desarrollo de la herramienta.

Para la estimación se usará el método de Puntos Casos de Uso (Use Case Points o UCP) desarrollado por Gustav Karner y está basado en la utilización de los casos de uso para la estimación. La razón de utilización de este método se debe a que es un método de estimación sencillo y eficaz y aprovechará los casos de uso que se definirán mediante UML en los capítulos siguientes.

Este método utiliza 4 factores para la realización de la estimación del esfuerzo:

- **Factor de peso de los actores sin ajustar (UAW):** Evaluación del número y la complejidad de los actores con los que interactuará el sistema.
- **Factor de peso de los casos de uso sin ajustar (UUCW):** Evaluación del número y la complejidad de los casos de uso del sistema.
- **Factor de complejidad técnica (TCF):** Evaluación del ajuste necesario basado en las características técnicas que presentará el sistema.
- **Factores de complejidad del entorno (ECF):** Evaluación del ajuste necesario basado en la complejidad del entorno al que se enfrentará el equipo de desarrollo.

### 6.2.1 Factor de peso de los actores sin ajustar (UAW)

Este factor evalúa la complejidad de los actores con los que tendrá que interactuar el sistema. Se calcula en función de la cantidad de actores de cada tipo, la naturaleza del actor (persona u otro sistema) y la forma de interacción.

| Tipo de Interacción | Peso Asignado |
|---|---|
| **Simple** (a través de API) | 1 |
| **Media** (a través de protocolo) | 2 |
| **Compleja** (a través de interfaz gráfica) | 3 |

Para **el caso de la herramienta HIS-SGSI el cálculo del factor UAW tiene el valor 30**, ya que todos los actores accederán a través de una interfaz gráfica.

| Actor | Nº Casos de uso | Factor | UAW |
|---|---|---|---|
| **Usuario** | 7 | 3 | 21 |
| **Administrador** | 3 | 3 | 9 |
| **Total** | **10** | | **UAW = 30** |

### 6.2.2 Factor de peso de los casos de uso sin ajustar (UUCW)

Este factor evalúa la complejidad de cada caso de uso según el número de transacciones, clases o tablas de las que haga uso.

En el presente caso para calcular la complejidad de un caso de uso se debe determinar el número de transacciones, incluyendo los caminos alternativos. Se entiende por transacción a un conjunto de actividades atómicas, ejecutadas de manera unitaria, es decir se ejecutan todas ellas o ninguna

| Nº de Transacciones del Caso de Uso | Tipo | Peso |
|---|---|---|
| **menor o igual que 3** | Simple | 5 |
| **mayor o igual que 4 y menor que 7** | Medio | 10 |
| **mayor o igual que 7** | Complejo | 15 |

Para **el caso de la herramienta HIS-SGSI el cálculo del factor UUCW tiene el valor 130**, ya que la mayoría de los casos de uso serán complejos.

| Tipo de Caso de Uso | Nº Casos de uso | Peso | UUCW |
|---|---|---|---|
| **Simple** | 1 | 5 | 5 |
| **Medio** | 2 | 10 | 20 |
| **Complejo** | 7 | 15 | 105 |
| **Total** | **10** | | **UUCW = 130** |

### 6.2.3 Factor de complejidad técnica (TCF)

Este factor evalúa la complejidad ciertos aspectos técnicos del sistema a desarrollar.

A cada uno de los Factores Técnicos de la tabla siguiente se le asigna un valor de influencia en el proyecto entre 0 (no tiene influencia) a 5 (esencial), el valor 3 se considera una valor de influencia medio.

| ID | Descripción | Peso | Valor | Resultado | Justificación |
|---|---|---|---|---|---|
| **T1** | **Sistema distribuido** | 2 | 3 | 6 | No se trata de un sistema fuertemente distribuido, solamente dos componentes |
| **T2** | **Objetivos de rendimiento o tiempo de respuesta.** | 1 | 3 | 3 | El rendimiento es importante en la experiencia del desarrollo, sin embargo no es un objetivo del proyecto. |

| | | | | | |
|---|---|---|---|---|---|
| **T3** | **Eficiencia del usuario final** | 1 | 5 | 5 | Se busca la mayor eficiencia del usuario en el manejo de la herramienta |
| **T4** | **Procesamiento interno complejo** | 1 | 4 | 4 | El procesamiento interno es complejo debido a los cálculos de representación de los datos en gráficas y resúmenes. |
| **T5** | **El código debe ser reutilizable** | 1 | 3 | 3 | Es deseable que el código sea reutilizable, sin embargo no será un objetivo de la herramienta. |
| **T6** | **Facilidad de instalación** | 0,5 | 4 | 2 | La herramienta debe ser instalable de una forma fácil. |
| **T7** | **Facilidad de uso** | 0,5 | 5 | 2,5 | La facilidad de uso de la herramienta en el proceso de un SGSI es un objetivo principal del desarrollo. |
| **T8** | **Portabilidad** | 2 | 2 | 4 | Sería deseable cierta portabilidad en el backend (SQL) pero no se considera bloqueante. |
| **T9** | **Facilidad para incorporar nuevos cambios** | 1 | 4 | 4 | Es importante preparar el desarrollo para que admita nuevas funcionalidades y cambios en la normativa sin grandes impactos |
| **T10** | **Concurrencia** | 1 | 3 | 3 | Se desea una concurrencia media. |
| **T11** | **Se incluyen objetivos especiales de seguridad** | 1 | 4 | 4 | El desarrollo debe incorporar medidas de seguridad por la naturaleza de los datos que debe manejar. |
| **T12** | **Provee acceso directo a terceras partes** | 1 | 0 | 0 | No aplica |
| **T13** | **Se requiere facilidades especiales de entrenamiento a los usuarios** | 1 | 0 | 0 | No aplica |
| **TOTAL** | | | | **TFactor= 40,5** | **TCF = 1,005** |

Obtenidos los grados de influencia se multiplican por el peso de cada factor y con la siguiente fórmula se calcula el Factor de Corrección Técnico que aplica al desarrollo.

**Para la herramienta HIS-SGSI se obtiene un valor TCF = 1,005**

### 6.2.4 Factor de complejidad del entorno (ECF)

Este factor evalúa la complejidad ciertos aspectos inherentes al entorno del sistema a desarrollar.

A cada uno de los Factores del Entorno de la tabla siguiente se le asigna un valor de influencia en el proyecto entre 0 (no tiene influencia) a 5 (esencial), el valor 3 se considera una valor de influencia medio.

| ID | Descripción | Peso | Valor | Resultado | Comentarios |
|---|---|---|---|---|---|
| **E1** | **Familiaridad con el modelo de ciclo de vida utilizado** | 1,5 | 3 | 4,5 | Se conoce el modelo utilizado |
| **E2** | **Experiencia en el ámbito de negocio** | 0,5 | 4 | 2 | El desarrollador conoce el ámbito de la seguridad |
| **E3** | **Experiencia en las metodologías de desarrollo utilizadas** | 1 | 3 | 3 | Se dispone de experiencia media en VB .Net y SQL |
| **E4** | **Capacidad del analista** | 0,5 | 3 | 1,5 | Se asume un analista de capacidad media |
| **E5** | **Motivación del equipo** | 1 | 3 | 3 | Se asume un equipo de con motivación media |
| **E6** | **Estabilidad de los requisitos** | 2 | 3 | 6 | Se asume una estabilidad media de los requisitos |
| **E7** | **Personal a tiempo parcial** | -1 | 0 | 0 | No habrá personal a tiempo parcial |
| **E8** | **Dificultad del lenguaje de programación** | -1 | 1 | -1 | El lenguaje de programación VB .Net/SQL no es especialmente difícil y existe numerosa documentación al respecto. |
| **TOTALES** | | | | **EFactor = 19** | **ECF=0,83** |

Obtenidos los grados de influencia se multiplican por el peso de cada factor y con la siguiente fórmula se calcula el Factor de Corrección Técnico que aplica al desarrollo.

**Para la herramienta HIS-SGSI se obtiene un valor ECF = 0,83**

### 6.2.5 Estimación de esfuerzo y coste

Con los datos anteriores y mediante la siguiente fórmula se calculas los puntos de casos uso:

**Para la herramienta HIS-SGSI se obtiene un valor de 134 puntos de caso de caso de uso o UCP**

$$UCP = (130 + 30) * 1{,}005 * 0{,}83 \approx 134$$

**Calculando 20 horas/hombre de esfuerzo por UCP y redondeando hacia la cifra entera superior se obtiene un total de 134 * 20 ≈ 2700 horas de tiempo de desarrollo.**

El tiempo total de desarrollo se repartirá de manera aproximada la siguiente manera:

| Actividad | Porcentaje |
|---|---|
| **Planificación y dirección** | **7,5%** |
| **Análisis** | **17,5%** |
| **Diseño** | **20%** |
| **Programación** | **40%** |
| **Pruebas** | **15%** |

Sobre esta estimación de 2700 horas y basándose en la distribución anterior se realiza la siguiente estimación del gasto con una aproximación del precio por hora de cada perfil lo que resulta en un **coste total estimado de 71750 euros para la herramienta HIS-SGSI.**

| Perfil | Funciones | Horas | Coste Hora | Total |
|---|---|---|---|---|
| **Responsable de proyecto** | El responsable del proyecto asigna los recursos, gestiona las prioridades, coordina las interacciones con los clientes y usuarios, y mantiene al equipo del proyecto enfocado en los objetivos. También establece un conjunto de prácticas que aseguran la integridad y calidad de los artefactos del proyecto y se encargará de supervisar el establecimiento de la arquitectura del sistema, la Gestión de riesgos, la planificación y control del proyecto. | 200 | 40,00 € | 8.000,00 € |
| **Ingeniero software** | Gestión de requisitos, gestión de configuración y cambios, elaboración del modelo de datos, preparación de las pruebas funcionales, elaboración de la documentación. Elaborar modelos de implementación y despliegue. | 300 | 35,00 € | 10.500,00 € |
| **Analista de sistemas** | Captura, especificación y validación de requisitos, interactuando con el cliente y los usuarios mediante entrevistas. Realiza la elaboración del Modelo de Análisis y Diseño. Colaboración en la elaboración de las pruebas funcionales y el modelo de datos. | 250 | 35,00 € | 8.750,00 € |
| **Consultor tecnológico** | Especialista en aspectos técnicos tales como interfaces de usuario, lenguajes de programación, metodologías y buenas prácticas en desarrollo, almacenamiento de datos, interacción y conectividad entre sistemas e implantación de verificaciones automatizadas de la seguridad en sistemas. | 200 | 35,00 € | 7.000,00 € |

| | | | | |
|---|---|---|---|---|
| **Consultor de seguridad** | Especialista en aspectos tales como seguridad, análisis de riesgos, estándares (ISO 27001, ISO 27002) y gestión de implantación de controles de cumplimiento de las mismas | 250 | 30,00 € | 7.500,00 € |
| **Programador #1** | Tareas de construcción de prototipos, colaboración en la elaboración de las pruebas funcionales, modelo de datos y en las validaciones con el usuario. | 750 | 20,00 € | 15.000,00 € |
| **Programador #2** | Tareas de construcción de prototipos, colaboración en la elaboración de las pruebas funcionales, modelo de datos y en las validaciones con el usuario. | 750 | 20,00 € | 15.000,00 € |
| **Totales** | | **2700 horas** | | **71.750,00 €** |

Para acelerar el tiempo de construcción y las pruebas del prototipo se decide repartir la tarea de programación entre dos programadores.

Esto mejoraría el tiempo de entrega ya que ambas tareas pueden ser realizadas en paralelo por los dos programadores según se aprecia en el diagrama de Gantt de la planificación correspondiente al desarrollo de la herramienta, ajustado a los recursos detallados anteriores.

| | Nombre | Trabajo | Duración | Inicio | Terminado |
|---|---|---|---|---|---|
| 1 | Gestión del Proyecto | 228 horas | 285 days | 2/01/12 8:00 | 1/02/13 17:00 |
| 2 | Fase de Análisis | 480 horas | 60 days | 2/01/12 8:00 | 23/03/12 17:00 |
| 3 | Fase de Diseño | 560 horas | 70 days | 26/03/12 8:00 | 29/06/12 17:00 |
| 4 | Fase de Construcción | 1.080 horas | 135 days | 2/07/12 8:00 | 4/01/13 17:00 |
| 5 | Fase de Pruebas y Evaluació | 400 horas | 50 days | 26/11/12 8:00 | 1/02/13 17:00 |



## 6.3 METODOLOGÍA DE DESARROLLO DE LA HERRAMIENTA

En los siguientes apartados se expondrán las metodologías, herramientas y procedimientos utilizados en el desarrollo de una herramienta que cubra todo el proceso de implantación de un SGSI expuesto en la primera parte del presente documento.

Para el proceso de desarrollo de la herramienta se optó por u**n modelo de prototipos sucesivos basado en un modelo de cascada resumido. La razón principal es alcanzar el objetivo de conseguir un producto utilizable en el menor tiempo posible y que pueda ser de utilidad al cliente**.

Las fases de este modelo son las siguientes:

- **Fase de análisis:** En esta fase **se expondrán los objetivos a cubrir con la misma junto con los requisitos necesarios para cubrir dichos objetivos y los datos que manejará la herramienta**. Se da la particularidad que aunque se siga el modelo de prototipado se extendió el proceso de determinación de objetivos y análisis requisitos más de lo que es habitual en una metodología de prototipos sucesivos, ya que se consideró que en este caso el cumplimiento estricto y con calidad de un conjunto limitado de requisitos iniciales en el prototipo inicial serviría para ofrecer al cliente confianza sobre el producto final.
- **Fase de diseño:** En esta fase los requisitos se definieron en los casos de uso y se establece el modelo de datos relacional que dará soporte al repositorio de datos. **Para ello se utilizará representación UML, Diagramas de Flujo de Datos (DFD) y diagramas entidad-relación para el modelado de datos**. Por otro lado y dada la necesidad de agilidad en el desarrollo en esta fase.se prescindieron de representaciones complejas como cronogramas o diagramas de clases.
- **Fase de desarrollo del prototipo:** En esta fase se implantaron los casos de uso y el modelo de datos en una serie de tecnologías definidas lo que resulta en un **prototipo de tipo vertical** (según lo expuesto por J. Nielsen relativo a las características de los prototipos[1]), es decir, un prototipo usable y elaborado que incluya un diseño refinado de la base de datos, de los interfaces del sistema y con un reflejo completo de los requisitos y rendimiento aceptable. Del mismo modo que en la fase anterior para agilizar esta fase se prescindieron de los detalles en la implementación de las clases.
- **Fase de evaluación del prototipo:** En esta fase se realizan las pruebas y se recogen las impresiones y mejoras propuestas del usuario y se verifican que se cumplen los requisitos solicitados mediante un plan de pruebas mínimo. Después se evalúan los datos recogidos y las decisiones se pasan a la fase siguiente.
- **Fase de mejora del prototipo:** En esta fase se analiza la viabilidad de la incorporación las mejoras propuestas del usuario de la fase anterior. De ser así se inicia un nuevo ciclo que permitirá obtener un nuevo prototipo.

**En el presente documento se centrará en las tres primeras fases y se comentará brevemente el desarrollo de las dos últimas ya que actualmente ya se dispone del producto una vez desarrollado, mejorado y evolucionado tras varias iteraciones del ciclo de desarrollo de los prototipos.**

## 6.3.1 FASE DE ANÁLISIS

### 6.3.1.1 Objetivos generales a cubrir con la herramienta

[1] Nielsen, J. (1993*). Usability Engineering*.

En los apartados siguientes se fijarán de manera general las funcionales y características que dispondrá la herramienta conforme a lo expuesto en la motivación del desarrollo de la herramienta expuesto en el apartado anterior:

- **OBJ-1: Soporte a la gestión de implantación de controles o salvaguardas** definidos en el estándar ISO/IEC 27002.2005 pudiendo controlar en todo momento el estado actual de conformidad. Posibilidad de gestionar otros posibles marcos normativos como RD 1720/2007, ENS (RD 3/10)... etc. Mantenimiento de información histórica, con posibilidad de revisar la mejora y evolución en el tiempo del estado de la seguridad.
- **OBJ-2: Gestión de indicadores de eficacia** de la implantación de los controles y su evolución en el tiempo
- **OBJ-3: Gestión y Registro de auditorías**. Seguimiento de las inconformidades y acciones correctivas pertinentes.
- **OBJ-4: Soporte al desarrollo y gestión del marco normativo documental de la organización** a implantar en la organización como requisito del SGSI.
- **OBJ-5: Definición y seguimiento de proyectos**, agrupando controles y comprobando en cado momento el nivel de implantación y su evolución en el tiempo.7

Representando de manera gráfica los cinco objetivos descritos obtendríamos un diagrama similar al siguiente que expande el elemento central HIS-SGSI del diagrama de contexto expuesto en el apartado MOTIVACIÓN DEL DESARROLLO DE LA HERRAMIENTA

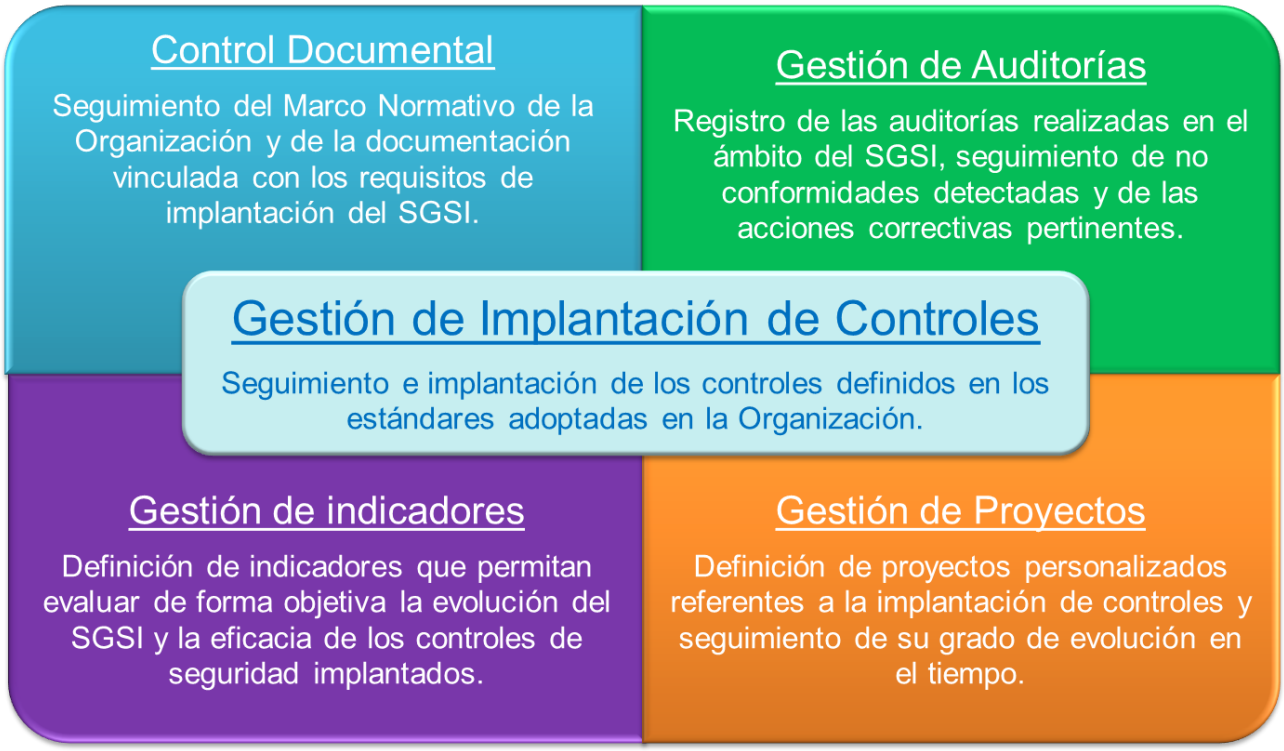



**Ilustración 18: Diagrama de nivel 2 de la herramienta**

Por otra parte no son objetivos de la herramienta ya que para ello se utilizarán otras herramientas más apropiadas:

- Soportar el proceso de análisis de riesgos inicial.
- Soportar el catálogo de activos de información de la organización.
- El cálculo del riesgo que soporta la organización en cada uno de los activos de información
- La herramienta tampoco pretende ser un gestor documental, y solamente se utilizará para el seguimiento y comprobación de cumplimiento del marco normativo y documental.

#### 6.3.1.2 Requisitos detallados de la herramienta

Se desglosan los objetivos y funciones de la herramienta descritos anteriormente en requisitos detallados que deben incorporarse al prototipo final:

| REQUISITO | OBJETIVO | DESCRIPCION |
|---|---|---|
| **RF-1** | **OBJ-1** | Dar soporte informático a la implantación de los estándares UNE-ISO/IEC 27001 y el catálogo de controles y buenas prácticas expuesto en ISO/IEC 27002 2005 y su estructuración en los niveles adecuados, mediante el seguimiento del nivel de madurez de implantación de las salvaguardas o controles en la organización. |
| **RF-2** | | Optativamente también dará soporte a otros marcos normativos nacionales e internaciones como RD 1720/2007, ENS (RD 3/10) etc. siempre que se ajusten a una estructura similar a ISO 27002:2005. El catálogo de controles no podrá ser manipulado por los usuarios de la herramienta a través de interfaces de usuario. |
| **RF-3** | | El sistema permitirá en todo momento controlar el estado actual de conformidad conforme al estándar o norma y mantendrá la información histórica que permita la posibilidad de revisar la mejora y evolución en el tiempo del estado de la seguridad. |
| **RF-4** | | Para organizaciones que deseen realizar la gestión de los controles con un nivel mayor de detalle se permitirá optativamente la definición e implantación de procedimientos de verificación detallados (tanto genéricos como personalizados para cada organización) de los controles o salvaguardas. |

| | | |
|---|---|---|
| **RF-5** | | La herramienta permitirá la utilización de un formato normalizado que permita la posibilidad de su incluir en la herramienta los resultados asociados a verificaciones automáticas de cumplimiento de los controles.<br><br>A este respecto la herramienta no realizará el proceso de comprobación automática, sino que permitirá la importación de los resultados en el formato definido. |
| **RF-6** | **OBJ-2** | La herramienta permitirá la gestión y definición de las métricas de indicadores personalizados para cada organización, así como la gestión de los resultados obtenidos en las métricas y su evolución en el tiempo. |
| **RF-7** | **OBJ-3** | Gestión y Registro de auditorías. La herramienta debe permitir el alta de auditorías referidas al cumplimiento de controles o a cualquier otro criterio que implique un impacto a la seguridad de la organización. También debe permitir el seguimiento en el tiempo de las inconformidades encontradas y las acciones correctivas pertinentes. |
| **RF-8** | **OBJ-4** | Permitir la gestión de cumplimiento del marco normativo y documental de las diferentes organizaciones. |
| **RF-9** | **OBJ-5** | Permitir planes de proyectos vinculados al seguimiento y evolución del estado de la implantación de los controles de tal manera que permita el agrupamiento de la implantación de controles. |
| **RF-10** | **TODOS** | La herramienta debe funcionar en modo multi-organización de modo que sea posible realizar el seguimiento de los datos de la evolución del cumplimiento de estándares de seguridad entre las distintas organizaciones incluidas en la herramienta y un usuario perteneciente a una organización no pueda visualizar los datos de otra organización. |
| **RF-11** | **TODOS** | La herramienta debe ser capaz de generar los siguientes listados e informes:<br><br>• Listados de los controles o salvaguardas y procedimientos de verificaciones de los anteriores y su estado actual. |

| | | |
|---|---|---|
| | | • Listados de los controles aplicables o no aplicables en la forma del informe de aplicabilidad de la organización.<br>• Listados de las no conformidades derivadas de las auditorías de los controles.<br>• Listados de métricas, así como un listado de los indicadores del sistema. |
| **RF-12** | **TODOS** | La herramienta debe ser capaz de generar de gráficas que permitan la visualización del estado actual de cumplimiento de los estándares así como su evolución en el tiempo de una manera intuitiva. |
| **RF-13** | **TODOS** | La herramienta debe contener las características de seguridad de autenticación y control de acceso de modo que permita una gestión de usuarios con las siguientes características:<br>• Autenticación autónoma / Autenticación integrada con repositorios centralizados de autenticación (Directorio Activo).<br>• Control de acceso a los datos por perfil de usuario y organización. |



#### 6.3.1.3 Datos manejados por la herramienta

El sistema debe ser capaz de manejar la información relativa a las siguientes:

- **Organización:** Entidad organizativa objetivo de seguimiento del nivel de seguridad en el marco de la implantación del SGSI (o no).
- **Activos**: Conjunto de elementos de la organización a proteger por el SGSI mediante la utilización de controles o salvaguardas. Puede ser cualquier tipo de activo de la organización afectado por el estándar de seguridad según lo definido por MAGERIT o cualquier otro definido por el usuario.
    - Servicios
    - Datos/Información
    - Aplicaciones (software)
    - Equipos informáticos (Hardware)
    - Redes de comunicaciones
    - Soportes de información
    - Equipamiento auxiliar
    - Instalaciones
    - Personal
    - Otros (Definidos por el usuario).

- **Estándar de seguridad**: Conjunto de normativas y recomendaciones reconocidas que conforman las directivas a seguir por la organización. El estándar se estructurará en **secciones**, que se componen de **apartados**, donde se ubican los **controles o salvaguardas de seguridad.**
- **Controles de seguridad**: Elemento final de los estándares, son objetivos para la mejora de la seguridad que afectan a cada uno a aspectos bien diferenciados. Los controles en cada organización poseerán un **nivel de madurez** basado en **revisiones del control** realizada por los responsables de la implantación del SGSI en función del estado de implantación de las **verificaciones** y un responsable de su implantación en cada organización.
- **Verificaciones:** Cada una de las comprobaciones que se realizan para la verificación de la correcta implantación un control de seguridad y de su estado de madurez. Las verificaciones contarán con una valoración de su nivel de implantación basado en la existencia de procedimientos de comprobación de la verificación y de los resultados obtenidos por su ejecución. Su **Grado de implantación c**onstituyen una instantánea del estado de implantación de las revisiones de los procedimientos a una fecha determinada. El estado de implantación de las verificaciones se calculará automáticamente de los resultados obtenidos al aplicar los procedimientos de comprobación. En caso que la verificación carezca de procedimientos de comprobación o de resultados el grado será **no evaluado**.
- **Procedimiento de comprobación de una verificación:** Los procedimientos son el desarrollo descriptivo del algoritmo de comprobación de una verificación aplicado a un activo (ver definición). La ejecución de un procedimiento puede ser manual o implicar el uso de herramientas adicionales. De la aplicación del procedimiento de comprobación se obtendrá un **resultado** indicando el grado de cumplimiento de la verificación. Se obtendrán los r**esultados de aplicar los procedimientos de comprobación y** son los indicadores del nivel de implantación de una verificación aplicado a un activo o poblaciones de activos en una fecha determinada.
- **Métricas:** Otras medidas definidas por el usuario para la mejora de la eficacia del SGSI y la seguridad de la información en una organización en un momento concreto. También se denominan registros.
- **Proyectos:** Proyectos de implantación de los controles del estándar. Se le debe poder asignar los datos necesarios para la planificación del proyecto, así como datos adicionales que permitan el seguimiento del mismo tal como el nivel de completitud del proyecto, responsables…etc.

- **Auditorías:** Las auditorías son revisiones a un departamento de una organización del nivel de implantación de los controles definidos en los estándares. Los resultados de la auditoría se denominan **hechos observados** en aquellos casos que exista una disconformidad con lo expuesto en el control y se dividen según su gravedad en **observaciones e incumplimientos**. En los casos que haya conformidad con lo expuesto en el control no se almacenará información al respecto en la auditoría. También existirá un histórico de las no conformidades de una auditoría que permita la visualización de su evolución en el tiempo.
- **Documentos:** Los documentos constituyen el marco normativo y documental de las diferentes organizaciones. Los documentos contienen los procedimientos e instrucciones técnicas de las verificaciones para los activos afectados. Para cada uno de los documentos se considerará, al menos, el tipo de documento (Política, Norma, Procedimiento…etc.) y el estado (Publicado, Pendiente, En revisión...etc.).

## 6.3.2 FASE DE DISEÑO

En esta fase se realizar el diseño de la herramienta de modo que cumpla con los objetivos y requisitos planteados en la fase de análisis anterior. Para ello se utilizará la definición de los casos de uso de la herramienta y los actores involucrados, el diagrama UML correspondiente a los casos de uso, los diagramas de flujos de datos en los casos que corresponda y el diagrama relacional del modelo de datos

### 6.3.2.1 Definición de actores de los casos de uso

Este apartado contiene los diferentes actores que se han identificado en la herramienta:

- **Nombre de actor:** Administrador

  **Descripción:** Este actor representa al perfil de administrador de la herramienta. Este tipo de usuarios puede realizar las acciones de gestión de la seguridad de una organización como un usuario no privilegiado y además tienen capacidad para realizar las siguientes acciones administrativas:
  - La gestión de los estándares en las herramientas y su vinculación a las organizaciones
  - La gestión de las organizaciones
  - La gestión de los usuarios no privilegiados
- **Nombre del actor:** Usuario

  **Descripción:** Este actor representa al perfil de usuario no privilegiado de la herramienta ya sea un consultor, un auditor, un empleado del área de seguridad o cualquier otro tipo de usuario involucrado con el SGSI o la seguridad en la organización. Este tipo de usuario puede realizar las acciones de gestión de la seguridad de una organización, pero no puede realizar las acciones privilegiadas de los usuarios administradores.

### 6.3.2.2 Diagrama de casos de uso

El siguiente diagrama muestra de manera general las funcionalidades de la herramienta, sus dependencias y sus relaciones con los actores principales de la herramienta: los usuarios cuyo principal objetivo será gestionar y obtener la información relativa al grado de seguridad en la organización.

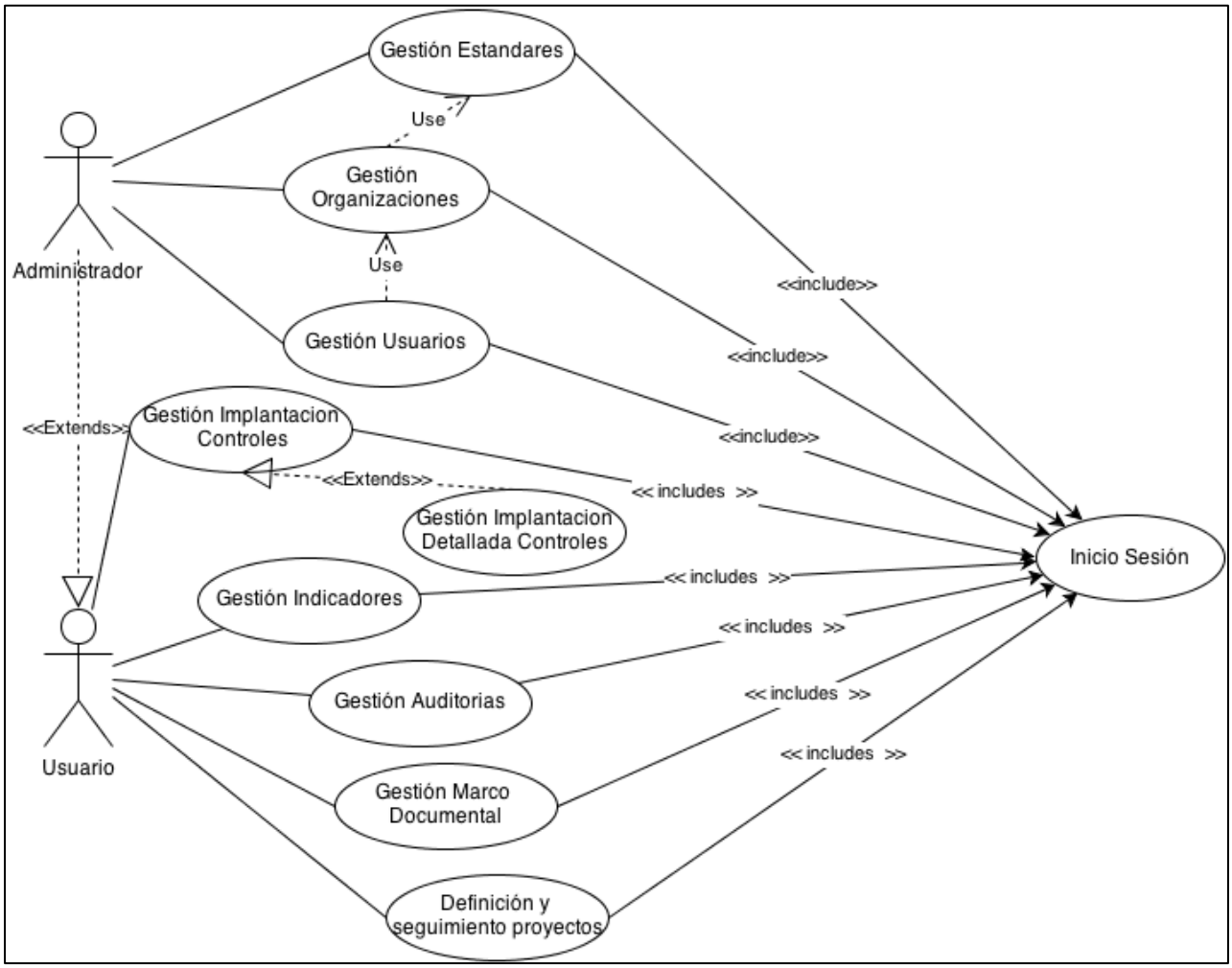



**Ilustración 19: Diagrama de casos de uso de la herramienta**

### 6.3.2.3 Caso de Uso: Gestión de los estándares

**Objetivos Asociados:**

- OBJ-1

**Requisitos Asociados:**

- RF-1
- RF-2

**Actores:**

- Usuario Administrador

**Descripción:**

La herramienta debe ser capaz de recoger, almacenar y gestionar los estándares manteniendo su estructura tal y como está reflejada en los documentos correspondientes. Principalmente el sistema se basará en la utilización del estándar ISO/IEC 27002 2005 aunque podría utilizar otros que se adaptaran a una estructura similar.

Solo el usuario administrador incluirá estándares en el sistema mediante la utilización de paquetes que incorporen todos los datos relativos a los estándares y su estructura.

Los datos relativos a los estándares vendrán precargados en la herramienta y no se permitirá que el usuario gestione directamente mediante interfaces de usuario los estándares existentes en el sistema (por ejemplo modificar controles de la ISO 27002) excepto por la incorporación de archivos XML correctamente formados con los datos relativos nuevos estándares.

Por lo tanto la herramienta no contempla las siguientes operaciones sobre los estándares:

- **Modificación de estándares a través del interfaz de usuario.**

*Estructura de los estándares*

Los estándares se estructuran en forma de árbol. Las entidades que forman los estándares son las siguientes (Las definiciones de cada una de las entidades descritas se encuentran en el apartado de descripción de los datos manejados por el sistema):

- **Repositorio**: Equivale a un estándar y se encuentra compuesto por una o varias secciones.
- **Sección**: Compuestas por uno o varios apartados relacionados.
- **Apartados**: Compuestos por uno o varios controles con un mismo objetivo.
- **Controles o salvaguardas**: Elementos objetivo de implantación.
- Aunque no se considere parte del estándar, optativamente podrá existir un proceso de **verificación genérica** del control que puede ser personalizado para cada organización (ver requisito RF-4 para más detalle).

El siguiente gráfico muestra de modo genérico la estructura en árbol de un estándar y las relaciones jerárquicas entre las entidades descritas.

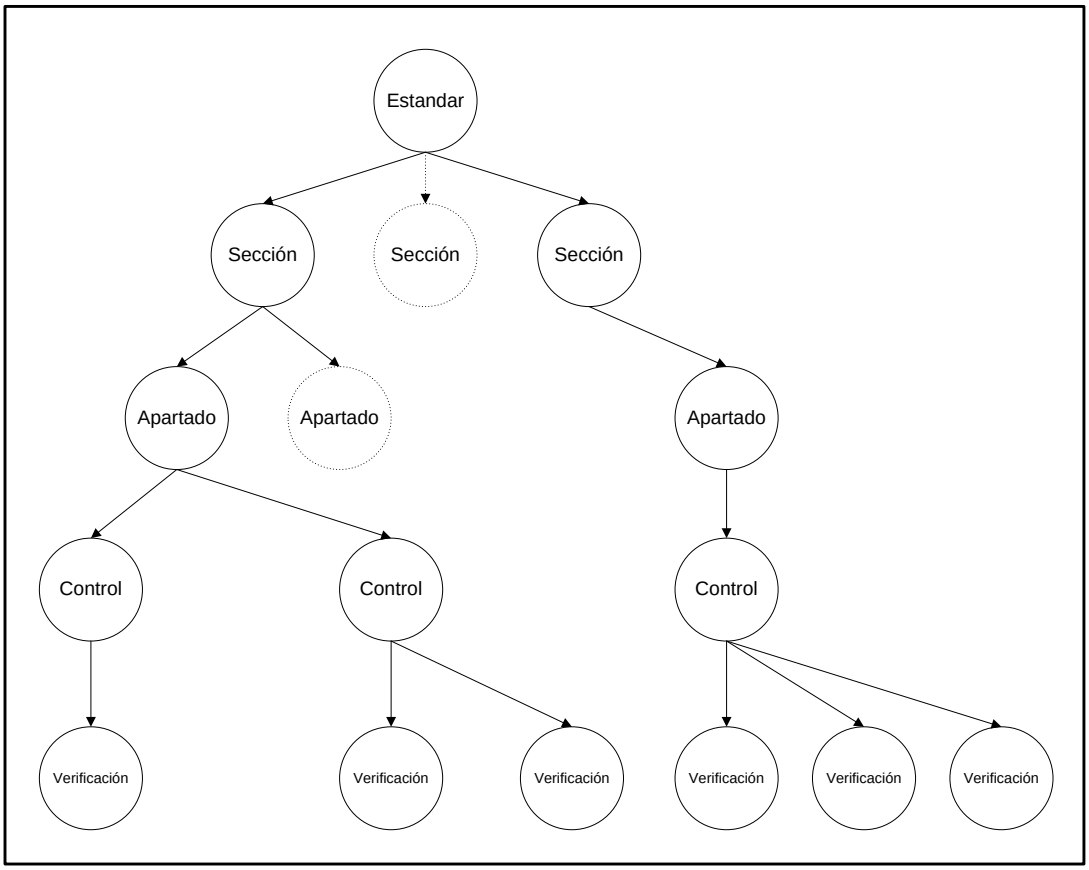



**Ilustración 20: Estructura en árbol de los estándares**

En el caso concreto del estándar ISO/IEC 27002:2005 se compone de:

- 1 Estándar
- 15 secciones
- 39 apartados
- 133 controles
- Un número indefinido de verificaciones a determinar para cada organización (optativo, al menos una para control aplicable).

#### 6.3.2.4 Caso de Uso: Gestión de organizaciones

**Objetivos Asociados:**

- Todos

**Requisitos Asociados:**

- RF-10

**Actores:**

- Usuario Administrador

**Descripción:**

La herramienta debe funcionar en modo "multiorganización", dado que se considera incluir funcionalidades que permitan comparar los datos de la evolución del cumplimiento de estándares de seguridad entre las distintas organizaciones incluidas en la herramienta.

La herramienta debe contener toda la información que permita realizar el seguimiento del SGSI de distintas organizaciones y de los distintos departamentos implicados. **Esta información solamente podrá ser suministrada por el usuario administrador que estará al cargo de la creación de la estructura de la organización por razones de seguridad impuestos por el cliente.**

Los datos a recoger de una organización serán los siguientes:

- Nombre de la organización.
- La descripción de la organización.
- El estándar o estándares a implantar en la organización.

Los datos a recoger de un departamento serán los siguientes:

- El nombre del departamento.
- La descripción del departamento.
- El responsable del departamento.
- La organización a la que pertenece.

Una vez una organización o departamento haya sido dada de alta no se permitirá su baja si tiene datos asociados.

#### 6.3.2.5 Caso de Uso: Gestión de usuarios

**Objetivos Asociados:**

- Todos

**Requisitos Asociados:**

- RF-13

**Actores:**

- Usuario Administrador

**Descripción:**

La herramienta debe mantener una gestión de los usuarios que permita un control de acceso mediante el uso de credenciales personales y los mecanismos de autenticación necesarios, así como los mecanismos necesarios para el control de acceso a los datos que contiene.

El identificador de usuario se utilizará de modo automático en las tablas históricas que así lo necesiten, lo que permitirá conocer el usuario que realizó los cambios.

Los datos a recoger de un cada usuario serán los siguientes:

- Identificador del usuario
- Nombre del usuario
- Repositorio de autenticación optativo
- Contraseña (en caso de autenticación local)
- Organización a la que pertenece.

Solamente el usuario administrador puede gestionar los usuarios de la herramienta aunque cada usuario podrá cambiar su propia contraseña en caso de autenticación local.

#### 6.3.2.6 Caso de Uso: Gestión de implantación de controles

**Objetivos Asociados:**

- OBJ-1

**Requisitos Asociados:**

- RF-1
- RF-3

**Actores:**

- Usuario

**Descripción:**

La herramienta permitirá asignar a los controles un seguimiento o revisión con un nivel de madurez lo que debe permitir realizar un seguimiento de la evolución de la madurez a nivel de control con carácter histórico.

La valoración del estado de implantación del control, dependerá del criterio del usuario y no de criterios como los resultados de las verificaciones (ver apartado siguiente), si bien estos resultados pueden servir como base al usuario para decidir el estado de implantación del control.

El gráfico siguiente muestra cómo el estado activo de la implantación de un control corresponde a la revisión del control de fecha más reciente, las revisiones anteriores quedan como histórico para el seguimiento de la evolución del estado de implantación del control.

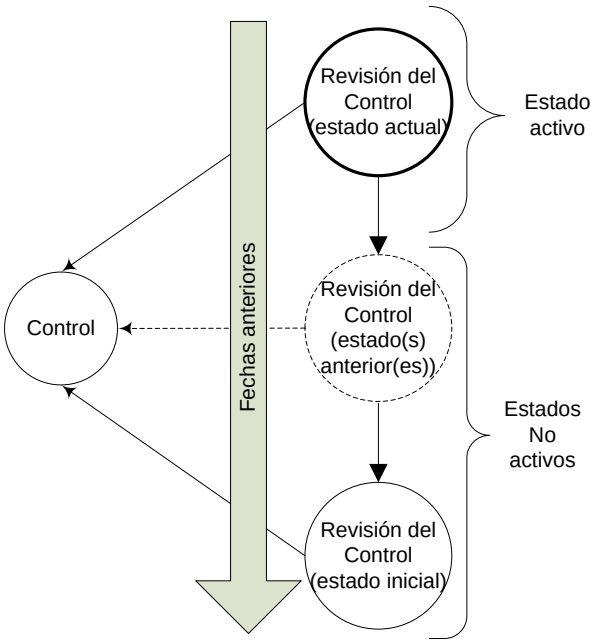



**Ilustración 21. Sucesivas valoraciones e histórico del estado del control**

#### 6.3.2.6.1 GESTIÓN DE LAS REVISIONES DE LOS CONTROLES

*Alta de revisiones de controles*

El alta de la revisión de un control permitirá la gestión de las revisiones de un control que tendrán los siguientes datos:

- **El estado del control:** Será determinado según el criterio del revisor y se corresponderá con los niveles de madurez CMM. Se deberán poder realizar nuevas revisiones de un control determinado. Como ayuda, la herramienta debería mostrar un listado con el estado de implantación de cada una de las verificaciones asociadas al control. Sin embargo, para determinar la madurez del control, el revisor también deberá conocer los procedimientos de comprobación definidos. El nivel de madurez asociado (CMM) lo determinará el revisor según su criterio de entre los siguientes:
  - **No aplicable:** El control no es aplicable a la organización **(Valor -2)**
  - **Aplicable:** El control es aplicable a la organización. Puede tener cualquiera de los siguientes estados
    - **Inexistente: (Valor 0)**
    - **Inicial: (Valor 1)**
    - **Gestionado: (Valor 2)**
    - **Definido: (Valor 3)**
    - **Cuantitativamente gestionado: (Valor 4)**
    - **Optimizado: (Valor 5)**
- **Justificación** del estado actual de aplicabilidad o no aplicabilidad

- **Comentarios asociados al control**. Estos irán precedidos (automáticamente) por la fecha de inserción del comentario. Se podrán añadir nuevos comentarios, pero no podrán ser borrados por el usuario.
- **Fecha de la última revisión** del control. Se actualizará automáticamente una vez modifique el estado del control. La revisión con la fecha más reciente se considerará la actual.
- **El departamento de la organización** asignado a la revisión del control.
- **Revisor que determinó** el nivel de madurez del control. Se tomará automáticamente del usuario que inició sesión.

*Modificación de las revisiones de los controles*

La única información que podrá modificar el usuario, una vez haya sido dado de alta el hecho observado será la siguiente:

- **El estado.** Se permitirá modificar el estado de los controles a las auditorías de manera libre y sin restricciones la transición de los estados. En caso de cambio del estado se debe almacenar toda la información referente al estado anterior para permitir el análisis histórico de la evolución del estado del control. **En el caso que existan varios estados relacionados con el mismo control se tomará como estado actual el de fecha más reciente y los anteriores se almacenarán a efectos históricos y de evolución del estado del control como se puede observar en el diagrama adjunto.**

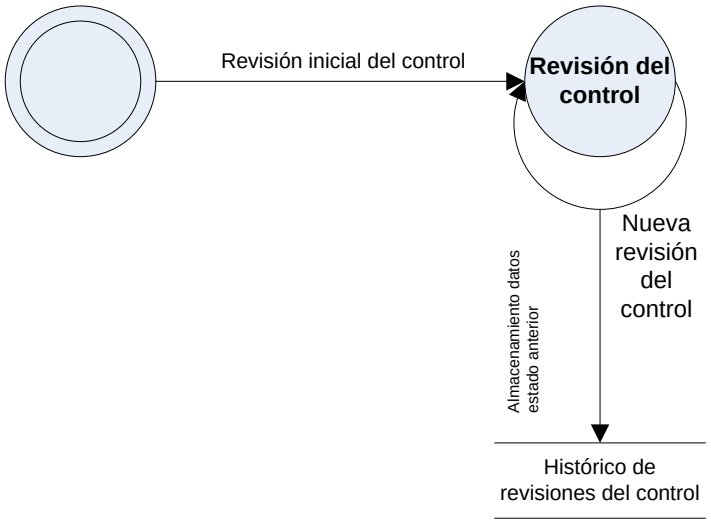



**Ilustración 22. Histórico de valoraciones del estado del control**

- **Justificación** del estado actual de aplicabilidad o no aplicabilidad.
- **Los comentarios:** El usuario podrá modificar los hechos observados dando de alta nuevos comentarios que no podrán ser borrados ni modificados por el usuario una vez introducidos.

*Modificación de las revisiones de los controles*

Se permitirá el borrado o baja de la revisión del control solamente en caso que no tenga almacenada información histórica de estados anteriores.

#### 6.3.2.7 Caso de Uso: Gestión de implantación detallada de controles

**Objetivos Asociados:**

- OBJ-1

**Requisitos Asociados:**

- RF-4
- RF-5
- RF-11
- RF-12

**Actores:**

- Usuario

**Descripción:**

Esta funcionalidad permitirá ampliar el detalle de la implantación de los controles a las organizaciones que así lo deseen de modo que la valoración del estado del control se base en los procedimientos de comprobación detallados y personalizados para cada organización.

El siguiente diagrama muestra la relación entre las normativas o estándares y los procedimientos de comprobación y el ámbito de aplicación en las diferentes organizaciones y puede ayudar al mejor entendimiento de las relaciones entre estas entidades.

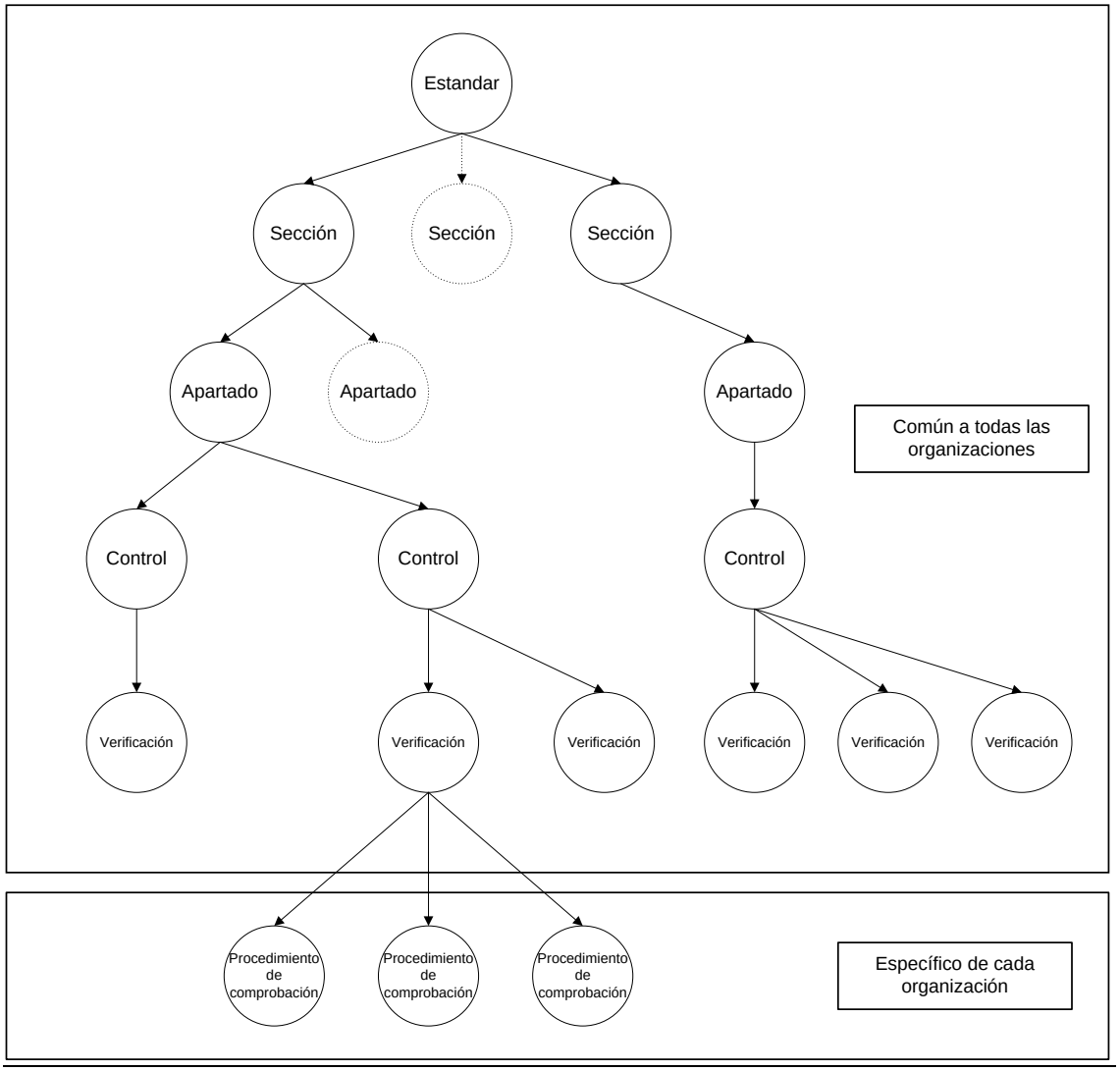



**Ilustración 23. Ámbitos de los estándares y de los procedimientos**

Cada revisión de un control tendrá un estado de madurez asignado por el consultor que se deberá basar en las valoraciones de las revisiones de las verificaciones asociadas a dicho control, que dependerá a su vez de los resultados de las comprobaciones de los procedimientos de verificación a una fecha determinada.

En el gráfico siguiente se muestra como la herramienta debe permitir realizar un seguimiento del **estado de los controles**, **estado de las verificaciones, los procedimientos de comprobación** y los resultados obtenidos al aplicarlos y el modo en que los resultados de los procedimientos de comprobación influyen en los resultados de las verificaciones pero los resultados de las revisiones de los controles son decididas por el usuario.

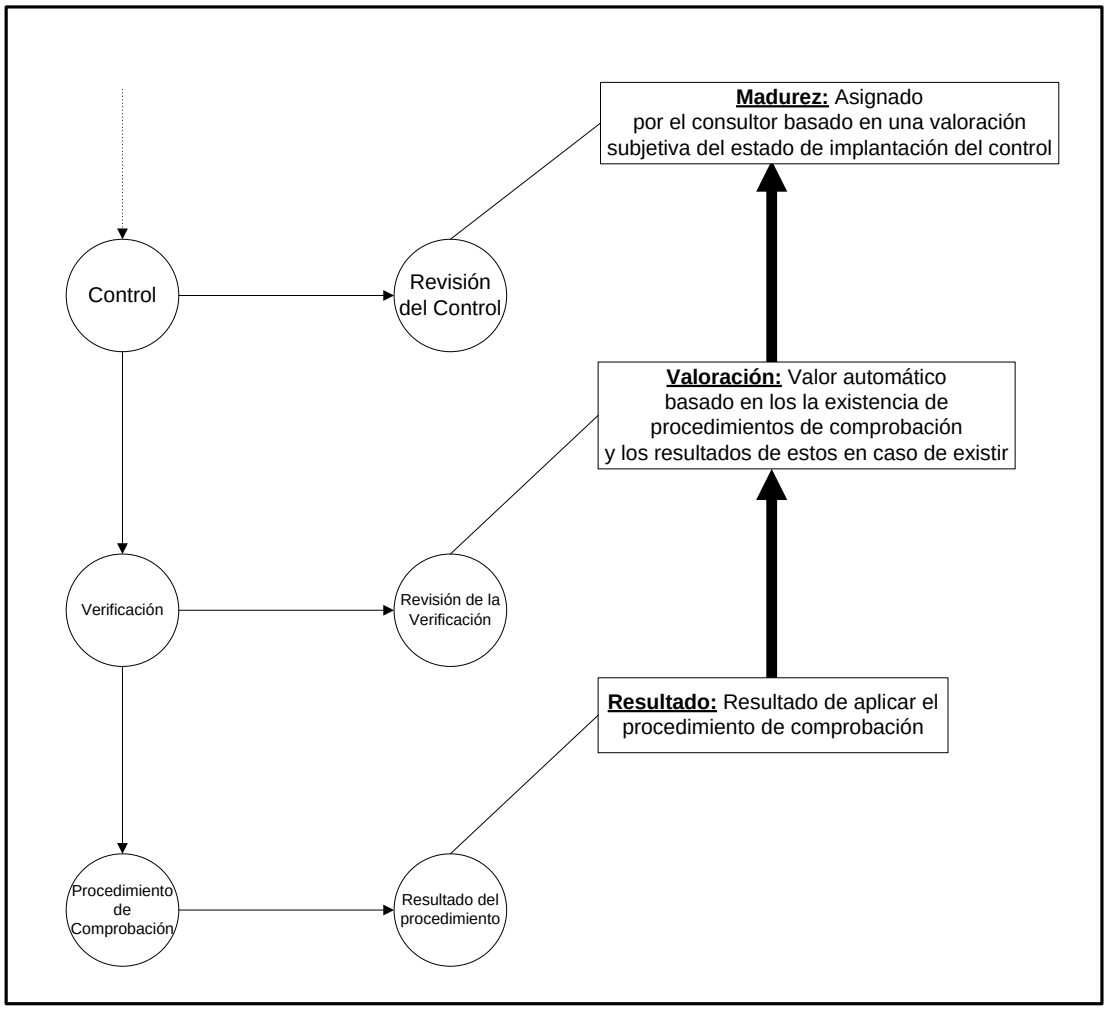



**Ilustración 24. Valoración de las entidades**

El estado de las verificaciones será determinado automáticamente por la herramienta y se obtendrá en función de los resultados recogidos de las ejecuciones de uno de sus procedimientos de comprobación por lo que no procede una gestión como tal sino que su estado depende de los resultados obtenidos de dichas ejecuciones.

La herramienta ofrecerá una valoración automática del estado de revisión de las verificaciones basado en la existencia de los procedimientos de comprobación y de los últimos resultados obtenidos de aplicar estos.

Las valoraciones posibles para las revisiones de las verificaciones en modo detallado serán las siguientes:

- **No aplica**: En el caso que la verificación encuentre en estado ***"No aplicable"*** o bien el estado actual del control del que depende sea ***"No aplica".***

- **Aplica**: En el caso de que los procedimientos de comprobación asociados se encuentren en estado “Activo”. Se debe ofrecer la fecha del último resultado en caso de existir y se contemplan los casos siguientes:
    - **No verificable**: Estado inicial, sin procedimientos de comprobación o sin resultados en los mismos.
    - **No implantado (No definitivo):** En el caso de que los últimos resultados de todos los procedimientos de comprobación hayan sido no satisfactorios y alguno de los procedimientos no tenga resultados.
    - **No implantado:** En el caso de que los últimos resultados de todos los procedimientos de comprobación hayan sido no satisfactorios.
    - **Parcialmente implantado (No definitivo):** En el caso de que últimos resultados en la ejecución de los procedimientos de comprobación sean tanto satisfactorios como no satisfactorios y además alguno de los procedimientos carezca de resultado.
    - **Parcialmente implantado:** En el caso de que últimos resultados en la ejecución de los procedimientos de comprobación sean tanto satisfactorios como no satisfactorios.
    - **Implantado:** En el caso que todos los últimos resultados obtenidos en la ejecución de todos los procedimientos de comprobación hayan sido satisfactorios.

La valoración de la revisión de las verificaciones se podrá obtener para el estado actual o para una fecha concreta, por lo que será necesario conservar el historial de los procedimientos de comprobación y de los resultados obtenidos al aplicarlos como se puede ver en el gráfico adjunto.

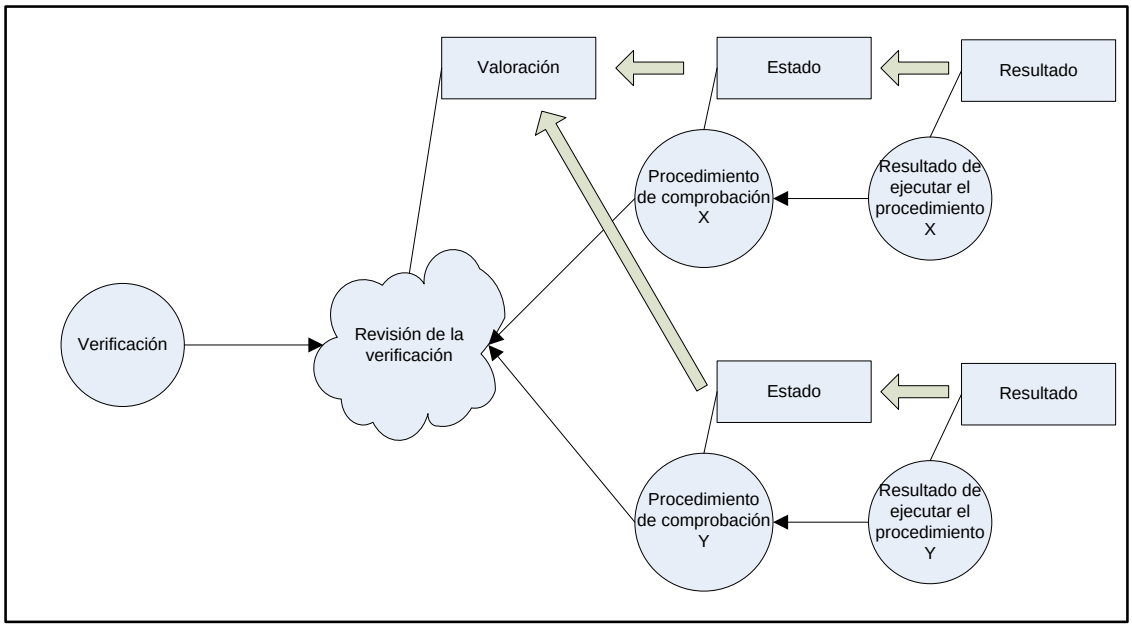



**Ilustración 25. Esquema de valoración de revisiones de las verificaciones**

#### 6.3.2.7.1 GESTIÓN DE LOS PROCEDIMIENTOS DE COMPROBACIÓN

*Alta de nuevo procedimiento de comprobación*

Se deberá permitir dar de alta nuevos procedimientos de comprobación para una verificación en concreto. El usuario deberá relacionar el nuevo procedimiento con, al menos, un documento del marco normativo, el cual debe haber sido dado de alta en la aplicación a través del gestor documental.

De los procedimientos de comprobación se debe poder recoger lo siguiente:

- **La verificación** a la que pertenece
- **La organización** al que pertenece el procedimiento
- **Descripción textual de las herramientas** empleadas.
- **Enlaces a documentos relacionados** como procedimientos o guías técnicas que deben ser dados de alta en la aplicación a través del gestor documental.
- **El activo donde se aplica** el procedimiento de comprobación.
- **Fecha de alta** del procedimiento (automático)
- **El estado** del procedimiento:
    - **Activo:** El procedimiento y sus resultados se deben tener en cuenta para la valoración de las revisiones de las verificaciones a la que pertenecen.
    - **No activo:** El procedimiento y sus resultados no se deben tener en cuenta para los resultados de las revisiones de las verificaciones a la que pertenecen. Es el estado inicial del procedimiento y el modo de dar de baja temporalmente un procedimiento de comprobación y sus resultados.

*Modificación de un procedimiento de comprobación*

Solamente se permitirá la modificación de procedimientos que no contengan resultados de los siguientes datos:

- **Descripción (textual) de las herramientas** empleadas.
- **Enlaces a documentos** relacionados.
- **El activo donde se aplica** el procedimiento de comprobación.

Se permitirá la modificación del siguiente atributo de los procedimientos que contengan resultados:

- El cambio del **estado (Activo / No activo) del procedimiento** ya que solamente afecta para la valoración de la revisión de las verificaciones.

En el caso de que se esté visualizando la última revisión realizada sobre un procedimiento de comprobación (es decir, la más actual), se deberá permitir crear una **nueva revisión del procedimiento de comprobación** que consistirá en crear un nuevo procedimiento de comprobación que sustituya al actual que pasará al estado **"No Activo"** como se muestra en el diagrama siguiente.

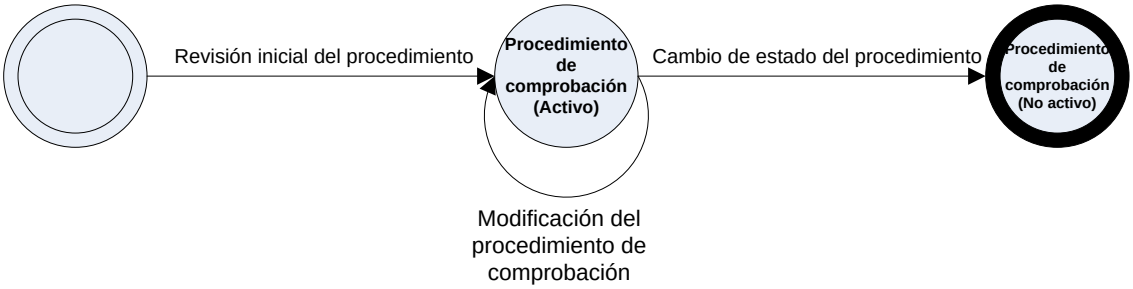



**Ilustración 26. Ciclo de vida de un procedimiento de comprobación**

*Baja de un procedimiento de comprobación*

No se contempla la baja de un procedimiento de comprobación. Para ello utilizar el estado activo o no activo en el procedimiento.

#### 6.3.2.7.2 GESTIÓN DE LOS RESULTADOS DE LOS PROCEDIMIENTOS DE COMPROBACIÓN

La herramienta debe permitir la gestión de los resultados de la ejecución de los procedimientos de comprobación de las revisiones.

*Alta resultado del procedimiento de comprobación*

La herramienta deberá permitir introducir nuevas ejecuciones de los procedimientos de comprobación definidos. En ellas se deberá especificar la siguiente información:

- **Procedimiento de comprobación al que corresponde** la ejecución.
- **Resultado de la ejecución del procedimiento** de comprobación. El estado de los resultados procedimientos de comprobación será determinado por el auditor en función de los resultados obtenidos. Los valores considerados son:
    - **Satisfactorio.**
    - **Parcialmente satisfactorio.**
    - **No satisfactorio.**

  En sucesivos resultados de la ejecución de un mismo procedimiento de comprobación se tomará como estado actual el de fecha más reciente y se almacenarán los anteriores resultados a efectos históricos y de evolución como se puede observar en el diagrama adjunto.

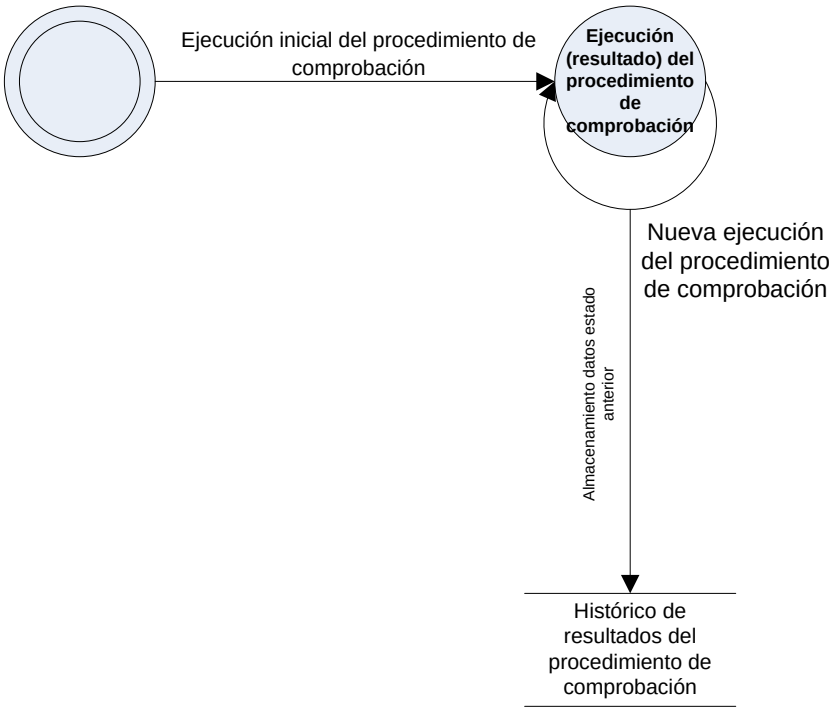



**Ilustración 27. Ciclo de vida de las ejecuciones de los procedimientos de comprobación**

- **Fecha de la ejecución** del procedimiento de comprobación.
- **Revisor encargado de la ejecución** del procedimiento de comprobación (por defecto el usuario de la herramienta).
- **Comentarios.**
- **Descripción textual de las evidencias** recogidas.
- **Normativa relacionada** con el procedimiento de comprobación, en caso de existir, sin embargo el revisor podrá añadir nuevos documentos si lo considera necesario.

*Alta resultados del procedimiento de comprobación desde otros sistemas*

La herramienta contará con un interfaz de datos normalizado y una utilidad de carga que permitirá al usuario incorporar los resultados de ejecutar procedimientos de comprobación automatizados provenientes de otros sistemas.

*Modificación resultado del procedimiento de comprobación*

La herramienta solamente permitirá las siguientes modificaciones:

- **Comentarios.**
- **Descripción textual de las evidencias** recogidas.

*Baja resultado del procedimiento de comprobación*

La herramienta no contempla la baja del resultado del procedimiento de comprobación.

#### 6.3.2.7.3 GENERACIÓN DE INFORMES Y LISTADOS

La herramienta debe generar los siguientes listados e informes referentesal estado de implantación del estándar.

- **Documento de aplicabilidad**: La herramienta debe permitir generar un listado con los controles y verificaciones aplicables y no aplicables con su justificación correspondiente para cada estándar que se pretenda implementar a la organización.
- **Documento de estado actual de controles:** La herramienta debe permitir generar un listado con el estado actual de implantación de los controles para cada estándar que se pretenda implementar a la organización.
- **Documento de estado actual de verificaciones**: La herramienta debe permitir generar un listado con el estado actual de las verificaciones (o procedimientos de comprobación) para cada estándar que se pretenda implementar a la organización.

#### 6.3.2.7.4 GENERACIÓN DE GRÁFICAS Y CUADROS DE MANDO

La herramienta debe generar las siguientes gráficas y cuadros de mando referentes estado de implantación para cada estándar que se pretenda implementar a la organización:

- **Gráficas de estado actual de controles:** Muestra el estado de madurez actual de los controles y la aplicabilidad.
- **Gráficas de evolución en el tiempo del estado de controles:** Muestra la evolución en el tiempo del estado de los controles entre dos fechas dadas.
- **Gráficas del estado actual de verificaciones:** Muestra el estado de implantación actual de las verificaciones y la aplicabilidad.
- **Gráficas de estado actual de procedimientos de comprobación:** Muestra el resultado de ejecución de los procedimientos de comprobación

### 6.3.2.8 Caso de Uso: Gestión de métricas e indicadores

**Objetivos Asociados:**

- OBJ-2

**Requisitos Asociados:**

- RF-6
- RF-11
- RF-12

**Actores:**

- Usuario

**Descripción:**

La herramienta permitirá al usuario definir las métricas numéricas que son indicativos del cumplimiento de objetivos en distintos aspectos de la seguridad y pueden ser definidos por los responsables de seguridad de la organización.

#### 6.3.2.8.1 GESTIÓN DE MÉTRICAS E INDICADORES

La herramienta debe permitir la gestión de las métricas para cada organización.

*Alta de indicadores*

La herramienta debe permitir dar de alta indicadores para el seguimiento del SGSI. De cada una de ellas se almacenará:

- **La descripción** textual.
- **La fórmula utilizada** descrita textualmente.
- **Fecha de alta:** Fecha de alta del indicador (automático).
- **Fecha de baja:** Fecha de baja del indicador (ver apartado de bajas).
- **Resultado esperado:** Valor esperado o deseable que debe tomar la métrica (debe ser un valor numéric**o).** Es el indicador del cumplimiento del objetivo.
- **Periodicidad de las mediciones** en meses**.**
- Opcionalmente podrán estar **vinculados a un control** de un estándar que permita realizar un seguimiento cuantitativo del mismo.

Se permitirá el alta del indicador sin el valor obtenido pudiendo añadirse posteriormente mediante la modificación. Una vez el valor obtenido se introduzca, el indicador quedará bloqueado para modificación.

*Modificación del indicador*

Se permitirá la modificación de la métrica solamente en el caso que no tenga resultado de los siguientes valores:

- **La descripción** textual.
- **La fórmula utilizada** descrita textualmente.
- **El control vinculado.**
- **Resultado esperado.**

*Baja del indicador*

Se permitirá la baja pero no el borrado del indicador que debe seguir siendo consultable a través de la herramienta. Para ello se permitirá introducir el siguiente dato:

- **Fecha de baja:** Fecha de baja de la métrica. En caso que el usuario realice la baja se asignará automáticamente la fecha actual como fecha de la baja.

#### 6.3.2.8.2 GESTIÓN DE RESULTADOS DE LAS MÉTRICAS

La herramienta permitirá asignar y modificar resultados o valores a las métricas definidas, siempre que no estén dadas de baja.

*Alta de resultados*

Se permitirán añadir los siguientes datos a un nuevo resultado de una métrica definida:

- **Fecha del valor:** Fecha que en obtuvo el resultado.
- **Valor esperado**: Una estimación del valor ideal a obtener.
- **Valor Obtenido:** Valor real obtenido al realizar la medición.

*Modificación de resultados*

Se podrán modificar los siguientes datos a un resultado existente:

- **Valor esperado**: Una estimación del valor ideal a obtener.
- **Valor Obtenido:** Valor real obtenido al realizar la medición.

*Baja de resultados*

No se contempla la baja de los resultados de la métrica una vez dados de alta.

#### 6.3.2.8.3 SEGUIMIENTO DE LOS RESULTADOS DE LAS MÉTRICAS

La herramienta debe permitir hacer un seguimiento de los valores recogidos en cada una de las métricas. El valor de la métrica con la fecha más reciente se considerará el valor actual del indicador.
Además debe ofrecer al usuario las siguientes funcionalidades:

- **Listado de estado de métricas**: La herramienta debe permitir generar un documento con la definición de todas las métricas existentes en la actualidad. Deberá incluir un anexo con aquellas que han sido dadas de baja, con una justificación. El valor concreto de cada métrica, también deberá ser recogido.
- **Gráfica de la evolución del indicador** y los valores de la métrica con respecto al tiempo.

### 6.3.2.9 Caso de Uso: Gestión de auditorías

**Objetivos Asociados:**

- OBJ-3

**Requisitos Asociados:**

- RF-7
- RF-11
- RF-12

**Actores:**

- Usuario

**Descripción:**

Las auditorias representan comprobaciones periódicas del cumplimiento de los controles del estándar que se pretende implantar en una organización o de otro tipo de comprobación aplicado a unos determinados departamentos de dicha organización y en un momento concreto.

La auditoría además recogerá información general relativa a la fecha, alcance, auditor que la realizó, el tipo de auditoría (interna o externa), si está aprobada y en tal caso el aprobador y un pequeño resumen de las conclusiones obtenidas. La herramienta también debe permitir recoger la información sobre auditorías realizadas y pendientes de realizar y el estado de las mismas.

Los resultados de la auditoría se denominan **hechos observados** que solamente existirán en aquellos casos en que exista una disconformidad con lo expuesto por el control o con otro tipo de comprobación. En los casos que haya conformidad, no existirá información al respecto ni otros datos relativos al cumplimiento del control. Los hechos observados se darán de alta y permitirán el cambio de estado, si bien debe quedar constancia del estado anterior del hecho no observados y de todos sus datos y del usuario que realizó el cambio a modo de histórico.

El sistema no contempla el seguimiento de los controles y verificaciones de cada auditoría. En todo caso la herramienta no asegura poder conocer el estado de implantación en el que se encontraba un control o verificación en una determinada auditoría.

#### 6.3.2.9.1 GESTIÓN DE AUDITORÍAS

*Alta de auditorías*

Se permitirá dar de alta nuevas auditorías en la herramienta. Será necesario que previamente se haya dado de alta el informe aprobado de resultados de la auditoría mediante el módulo de gestión documental y el departamento sobre el que se realiza la auditoría. Por tanto, se entiende que la auditoría debe haber finalizado y tener resultados o hechos observados.

En el alta de una nueva auditoría se recogerá la siguiente información:

- **El departamento** de la organización sobre el que se realiza.
- **Enlace al informe** de resultados de la auditoría, que debe haber sido dado de alta previamente en el módulo de gestión documental.
- **El tipo** de auditoría:
  - **LOPD**
  - **SGSI**
- **El origen** de la auditoría:
  - **Interno**
  - **Externo**
- **El estado** de la auditoría:
  - **No aprobada:** Valor por defecto.
  - **Aprobada:** Una vez se apruebe no se podrá modificar los datos de la misma.
- **Fecha de aprobación** de la auditoría**:** Optativo de manera inicial. Se debe introducir una vez cambie el estado a “aprobada”.
- **Fecha de** realización: Fecha de finalización de la auditoría (obligatorio).

- **El objetivo** de la auditoría, como una descripción textual.
- **Alcance** de la auditoría, como una descripción textual.
- **Auditor jefe** de la auditoría, como un texto libre. Por tanto se podría recoger el nombre de una persona, un departamento o una empresa.
- **Aprobador** de la auditoría, como un texto libre. Por tanto se podría recoger el nombre de una persona, un departamento o una empresa (obligatorio).
- **Comentarios** sobre el desarrollo de la auditoría como una descripción textual. Estos irán precedidos (automáticamente) por la fecha de inserción del comentario y no podrán ser borrados por el usuario.

Una vez el usuario haya introducido toda la información descrita en los puntos anteriores, se podrá dar de alta la nueva auditoría. Posteriormente se le podrán asignar los hechos observados correspondientes del informe de resultados.

El siguiente diagrama presenta el modelo de los estados y el ciclo de vida de los elementos que componen las auditorías.

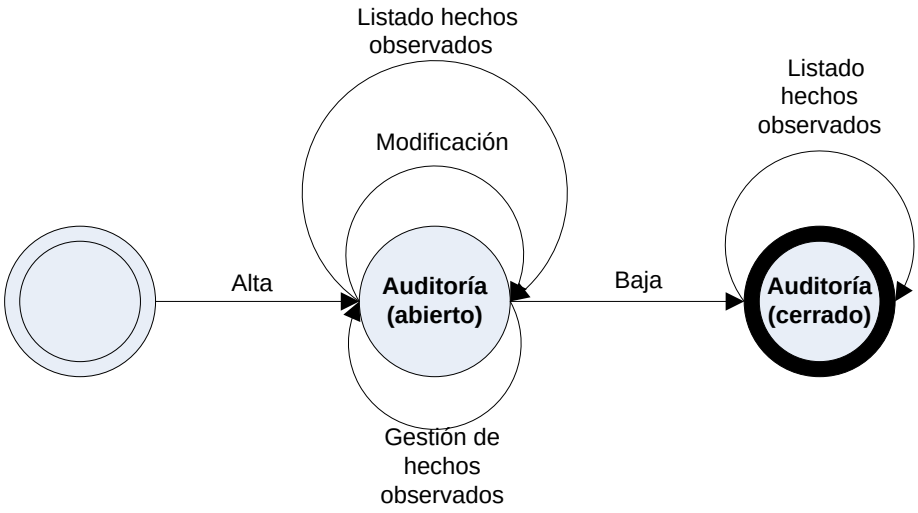



**Ilustración 28. Ciclo de vida de la auditoría**

*Modificación de auditorías*

La única información que podrá modificar el usuario, una vez haya sido dado de alta la auditoría, será la siguiente:

- **El objetivo de la auditoría.**
- **Alcance de la auditoría**.
- **Auditor jefe de la auditoría.**
- **Aprobador de la auditoría.**
- **Fecha de aprobación de la auditoría.**

- **Comentarios sobre el desarrollo de la auditoría** como una descripción textual. Estos irán precedidos (automáticamente) por la fecha de inserción del comentario y no podrán ser borrados por el usuario. El usuario podrá modificar dando de alta nuevos comentarios que no podrán ser borrados ni modificados una vez introducidos.

*Baja de auditorías*

No se contempla la baja de auditorías

#### 6.3.2.9.2 LISTADO DE AUDITORÍAS REALIZADAS

Se permitirá consultar un extracto de todas las auditorías dadas de alta en la herramienta. Para cada una de ellas se mostrará la siguiente información:

- **Tipo** de Auditoría**.**
- **Fecha de finalización** de la auditoría.
- Número de **hechos observados** que han sido **detectados** en la auditoría.
- Número de **hechos observados en cada uno de los estados posibles** de los detectados en la auditoría. (MY, MN, OBS, ODM) agrupados para cada tipo de auditoría (ver punto siguiente).

Además la herramienta debe permitir al usuario generar los siguientes listados:

- **Listado de no conformidades (agrupadas por estado):** La herramienta debe permitir generar un documento con todas las no conformidades agrupadas por el estado en el que se encuentran actualmente en la organización.
- **Listado de no conformidades (agrupadas por auditoría):** La herramienta debe permitir generar un documento con todas las no conformidades agrupadas por el estado en el que se encuentran actualmente en la organización.
- **Listado por auditoría**: La herramienta debe permitir generar un documento de todos hechos observados por la auditoría en la que fueron detectadas, y deberá incluir información sobre el estado en el que se encuentran actualmente en la organización.

#### 6.3.2.9.3 GESTIÓN DE HECHOS OBSERVADOS EN AUDITORÍAS

Se permitirá asignar hechos observados o resultados no favorables a una auditoría que previamente haya sido dada de alta en la herramienta.

*Alta de los hechos observados*

La información que se recogerá para asignar hechos observados a una determinada auditoría es la siguiente:

- **La auditoría** a la que pertenece el hecho observado.
- **Tipo de hecho observado**: Las opciones el tipo dependerá del tipo de auditoría y se permitirá moverse libremente entre cualquiera de los estados. En el caso de que fuera de tipo “SGSI” serían, por orden de mayor a menor nivel de criticidad:

    - **MY**: No conformidad mayor. Constituye un incumplimiento grave.
    - **MN**: No conformidad menor. Constituye un incumplimiento leve.
    - **OBS**: Observación sobre un hecho observado. No significa incumplimiento.
    - **ODM**: Oportunidad sobre un hecho observado. No significa incumplimiento.
- **Estado del hecho observado.** Se permitirá moverse libremente entre cualquiera de los estados de entre los siguiente posibles, si bien se deberá guardar copia del estado actual antes de pasar al nuevo para permitir la consulta histórica:
    - **No iniciado**: No se ha iniciado la resolución del hecho observado.
    - **En proceso**: Se ha iniciado la resolución del hecho observado.
    - **Pendiente validación**: Se ha concluido la resolución del hecho observado pero está pendiente de validación por los responsables correspondientes.
    - **Cerrado**: Se ha concluido la resolución del hecho observado y ha sido validado por los responsables correspondientes.
    - **No válido**: Este estado implica un estado no válido del hecho observado.
- **Descripción del hecho observado y su causa** como una descripción textual. No se contempla el recoger la causa del hecho observado en un campo independiente.
- **Descripción de las acciones correctivas acordadas** como una descripción textual.
- **Responsable de resolución** como una descripción textual. Se podría recoger el nombre de una persona, un departamento o una empresa.
- **Responsable de revisión** como una descripción textual. Se podría recoger el nombre de una persona, un departamento o una empresa.
- **Fecha estimada de resolución.**
- **Fecha de modificación del hecho observado,** que inicialmente será la fecha en la que se produce la asignación a la auditoría.
- **Comentarios sobre el desarrollo de la auditoría** como una descripción textual. Estos irán precedidos (automáticamente) por la fecha de inserción del comentario y no podrán ser borrados ni modificados por el usuario una vez introducidos.
- **Optativamente se podrá relacionar el hecho observado con un control** de los estándares existentes en el sistema

El siguiente diagrama presenta el modelo de los estados y el ciclo de vida de los hechos observados que componen las auditorías.

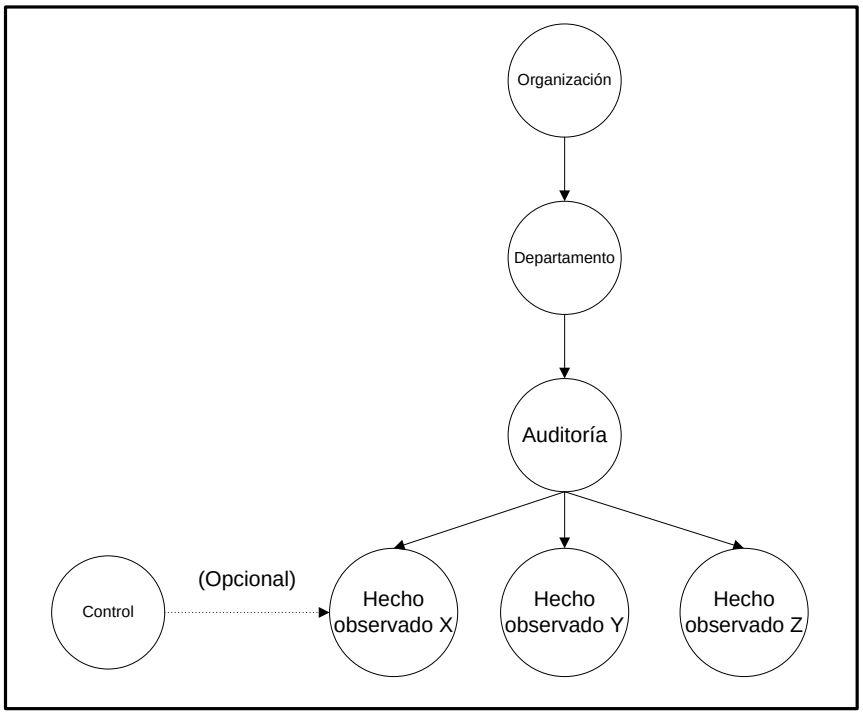
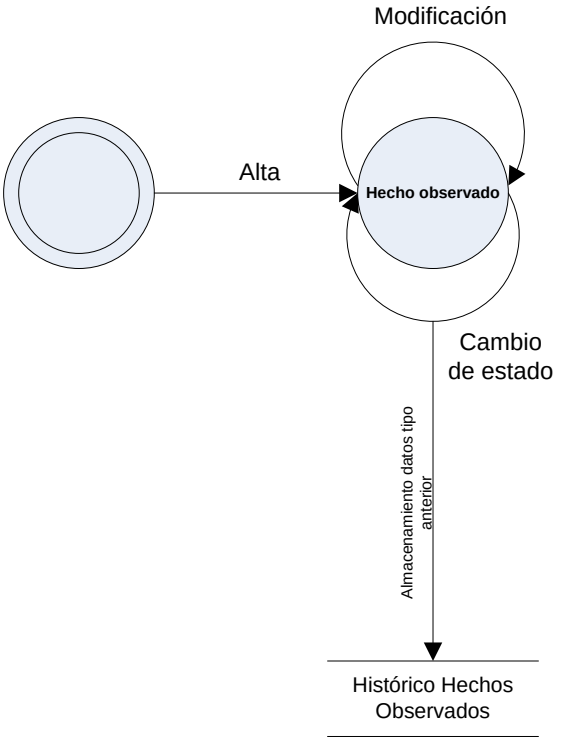



**Ilustración 29. Auditorías y hechos observados**

*Modificación de los hechos observados*

La única información que podrá modificar el usuario, una vez haya sido dado de alta el hecho observado, será la siguiente:

- **El estado.** Se permitirá modificar el estado de los hechos observados asignados a las auditorías de manera libre y sin restricciones la transición de los estados. En caso de cambio del estado se debe almacenar el estado anterior para la consulta con carácter histórico de la evolución del hecho observado según se puede observar el en gráfico siguiente.




- **Comentarios:** El usuario podrá modificar los hechos observados dando de alta nuevos comentarios que no podrán ser borrados ni modificados por el usuario una vez introducidos.
- **Responsable de resolución** como una descripción textual. Se podría recoger el nombre de una persona, un departamento o una empresa.
- **Responsable de revisión** como una descripción textual. Se podría recoger el nombre de una persona, un departamento o una empresa.
- **Fecha estimada de resolución:** Una fecha estimada en la cual el hecho observado estará solventado.

*Modificación de los hechos observados*

Se permitirá el borrado o baja del hecho observado solamente en caso que no tenga almacenada información histórica de estados anteriores.

#### 6.3.2.10 Caso de Uso: Gestión del marco normativo y documental

**Objetivos Asociados:**

- OBJ-4

**Requisitos Asociados:**

- RF-8
- RF-11
- RF-12

**Actores:**

- Usuario

**Descripción:**

La herramienta debe poder permitir la gestión de cumplimiento respecto del estándar del marco normativo y documental de las diferentes organizaciones. Estos documentos podrán estar relacionados con procedimientos de comprobación. Para cada uno de los documentos que lo componen se considerará, al menos:

- **El tipo** de documento (Política, Norma, Procedimiento…).
- **El estado** de documento (Publicado, Pendiente, En revisión...).
- **El aspecto de la seguridad cubierto** por cada documento.

#### 6.3.2.10.1 GESTIÓN DE DOCUMENTACIÓN

*Alta de nuevos documentos*

Para cada uno de los documentos que lo componen se considerará, al menos los siguientes datos:

- El **título** del documento .
- La **descripción** del documento.
- **La versión** del documento.
- El **tipo** de documento:
    - Política.
    - Norma.
    - Procedimiento.
    - Instrucciones Técnicas.
    - Plantilla.
    - Revisión.
    - Acta.
- El **estado** del documento:
    - Obsoleto.
    - No Aplicable.
    - Pendiente.
    - Iniciado.
    - Pendiente Revisar.
    - Revisado.
    - Modificándose.
    - Pendiente Aprobación.
    - Aprobado.
    - Publicado.
- **Procedimientos de comprobación relacionados** con el documento**:** Será opcional y se podrán relacionar posteriormente. Los documentos dados de alta en la herramienta y que no estén en estado obsoleto podrán asociarse a uno o varios procedimientos de comprobación

- **Organización** a la que pertenece.
- **Enlace** al documento mediante un camino local, de red, URL...etc. El acceso a los documentos se realizará a través de enlaces. La herramienta no almacenará archivos, si no que deberán encontrarse en una unidad de red accesible al sistema donde está instalada la herramienta.

*Modificación de los documentos*

La modificación de los documentos dados de alta se permitirá en los siguientes datos:

- El **título del documento**
- La **descripción del documento**
- El **estado del documento**
- **Procedimientos de comprobación relacionados con el documento**
- **Enlace al documento**

Los documentos no podrán modificarse una vez tengan procedimientos de comprobación asignados. La actualización del contenido de los documentos dados de alta no será gestionada por la herramienta, dado que los ficheros se encontrarán ubicados en un repositorio independiente.

*Baja documentos*

Solo se podrán eliminar documentos del marco normativo, cuando no estén relacionados con ninguno de los procedimientos de comprobación existentes. En otros casos se utilizará el estado "**Obsoleto**" para indicar que el documento no se utilizará.

*Listado de documentos*

**Gráfica de estado actual de documentos:** La herramienta debe generar gráficas que permitan mostrar el estado de actual de los documentos.

#### 6.3.2.11 Caso de Uso: Gestión del plan proyectos de seguridad

**Objetivos Asociados:**

- OBJ-5

**Requisitos Asociados:**

- RF-9

**Actores:**

- Usuario

**Descripción:**

Para cada organización, la herramienta debe permitir definir un plan de proyectos. El plan de proyectos constará de una serie de proyectos estándar que se podrán planificar en el plazo que el usuario estime oportuno.

El usuario podrá asignar cada uno de los distintos proyectos a un plazo, las posibles opciones serán:

- Corto

- Medio
- Largo
- N/A: en caso de que no se planifique el proyecto

Para cada uno de los proyectos se deberá definir el nivel objetivo de cumplimiento que se desea alcanzar.

Los proyectos se relacionarán con los controles a través del cumplimiento de las verificaciones. Las relaciones entre los proyectos y las verificaciones no serán modificables por el usuario.

#### 6.3.2.12 Caso de Uso: Inicio de sesión

**Objetivos Asociados:**

- Todos

**Requisitos Asociados:**

- RF-13

**Actores:**

- Todos

**Descripción:**

La herramienta debe solicitar la autenticación del usuario que intenta acceder a cualquiera de las operaciones permitidas por la herramienta, bien a través de la introducción de la herramienta o través de cualquier otro tipo de autenticación previa.

### 6.3.3 Modelo de datos relacional

Se desarrolla el modelo de datos relacional que servirá como repositorio de la información gestionada por la herramienta.

El siguiente diagrama muestra las entidades y sus relaciones el modo en que finalmente se implementarán en la base de datos de la herramienta.

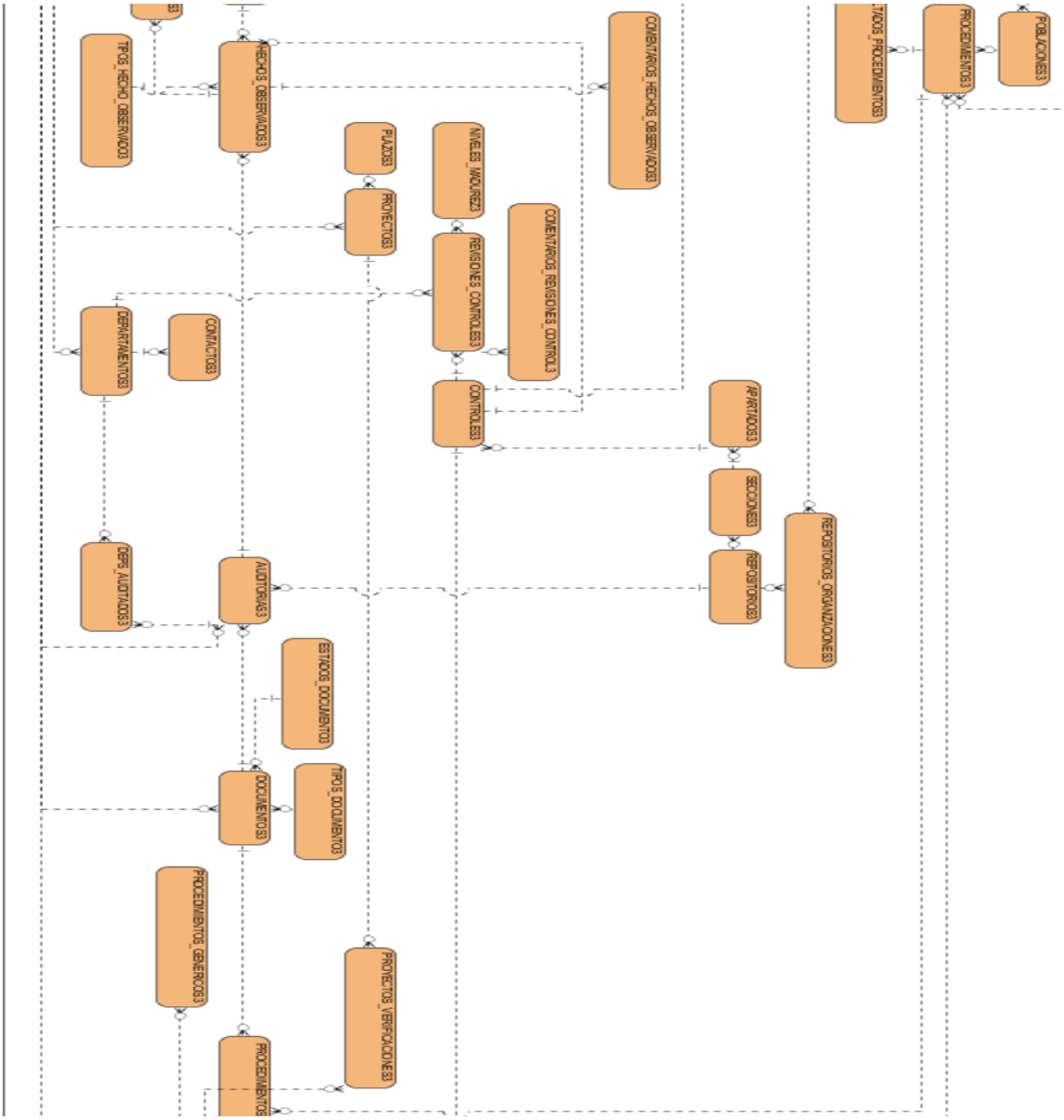



**Ilustración 30. Modelo de datos de la herramienta**

## 6.3.4 FASE DE DESARROLLO DEL PROTOTIPO

En este apartado se exponen los detalles técnicos y las tecnologías del proceso de desarrollo inicial de la herramienta.

### 6.3.4.1 Arquitectura objetivo

Se opta por una arquitectura cliente-servidor basado en un cliente pesado con un repositorio en base de datos relacional por las siguientes razones:

- No se espera una utilización masiva de la herramienta por parte de diversos usuarios.
- Simplifica la arquitectura y el despliegue del producto.
- No se necesita un acceso desde redes públicas por lo que no sería necesaria una arquitectura de tipo Web ni medidas de seguridad adicionales para evitar el acceso no permitido a los datos.

- Este tipo de arquitectura permite un mayor rendimiento al residir localmente.

#### 6.3.4.2 Interfaz de usuario

Para la **parte cliente del aplicativo de gestión o front-end** de usuario se utiliza una plataforma visual e intuitiva. En el caso presente el lenguaje **Microsoft Visual Basic**. Net mediante el interfaz de desarrollo Visual Studio Express 2008 por las siguientes razones:

- Satisface y facilita la implementación de la mayor cantidad de los requisitos planteados para las características no funcionales de la herramienta como los mecanismos de seguridad, el control de acceso a los datos, la integridad de datos, el soporte transaccional y el registro de actividad.
- Al hacer uso del Framework .Net 3.5 SP1 permite un desarrollo más rápido y ágil.
- Las plataformas Windows están ampliamente difundidas en el entorno empresarial.
- Permite la creación de interfaces de usuario e incorpora las librerías de acceso y presentación de datos así como de representación gráficos de manera rápida y sencilla.
- Permite una integración directa del entorno Visual Studio con el repositorio MS SQL Server lo que facilita y agiliza el proceso de desarrollo.
- Puede ser obtenido de manera gratuita desde la Web del fabricante Microsoft.

#### 6.3.4.3 Repositorio de datos

Para el **repositorio de los datos o back-end** se utilizará la base de datos relacional **MS SQL Server 2008 Express** las razones para esta decisión son las siguientes:

- Satisface y facilita la implementación de la mayor cantidad de los requisitos planteados para las características no funcionales de la herramienta como los mecanismos de autenticación, el control de acceso a los datos, la integridad de datos, el soporte transaccional, el acceso concurrente a los datos y el registro de actividad.
- Permite implantar los procesos internos de manipulación de los datos en forma de procedimientos almacenados y funciones y manejo de esquemas XML para la importación de datos.
- Permite una integración directa con el entorno Visual Studio y el lenguaje VB .Net lo que facilita y agiliza el proceso de desarrollo.
- Puede ser obtenida de manera gratuita desde la Web del fabricante Microsoft. Si bien las versiones Express tienen cierta limitación en el tamaño de las bases de datos, esta limitación es lo suficientemente alta para no presentar un impedimento en su utilización con la herramienta.
- Es posible instalarla en el puesto donde se instale la parte cliente de modo que el despliegue del sistema es más sencillo.
- Es completamente compatible con las versiones empresariales de MS SQL Server 2005, 2008 y superiores ya que estos productos suelen estar implantados de manera habitual en la mayoría de organizaciones.

#### 6.3.4.4 Arquitectura de la herramienta

La arquitectura que presentará la herramienta será de tipo cliente servidor, lo que permite que el despliegue sea rápido y no requiera la existencia de infraestructuras complejas. En caso de necesidad el repositorio de datos puede existir en el mismo sistema que el interfaz de usuario.

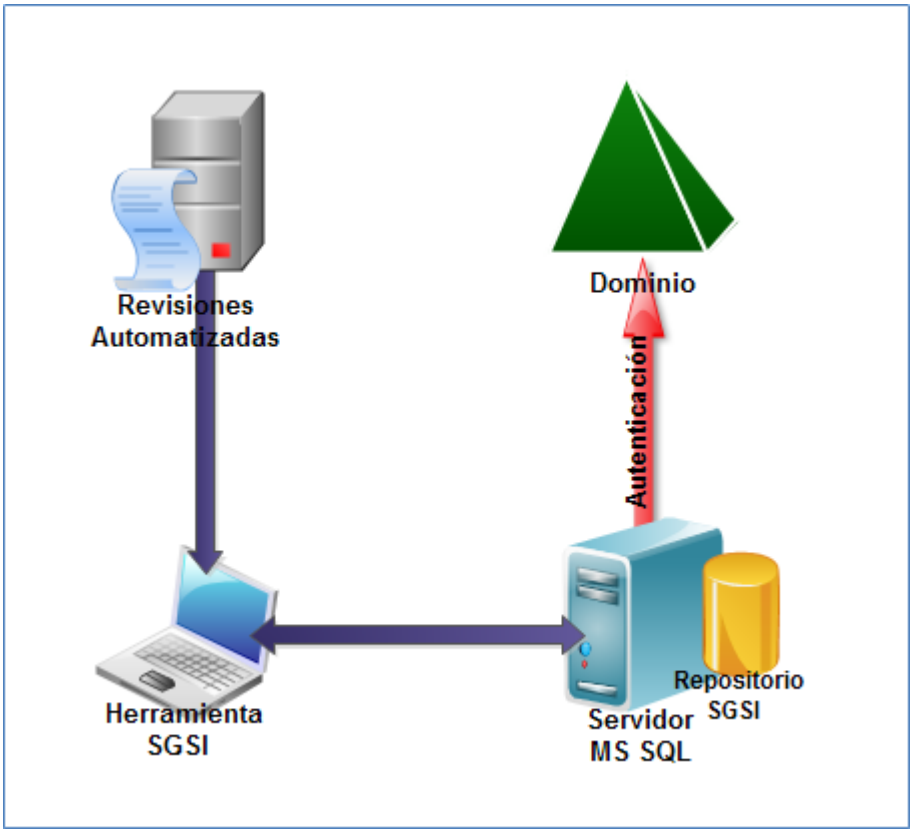



Ilustración 31. Arquitectura final de la herramienta

El software base y requisitos mínimos necesarios para la instalación de la herramienta el cliente serán el siguiente:

**Para el front-end o cliente de la herramienta**

- Hardware
  - Compatible con Pentium III o superior 1 GHz. o más.
  - 1 GB de memoria RAM.
  - Pantalla capaz de alcanzar al menos 1280 x 768 pixeles de resolución.
  - 1 GB de espacio libre en disco.
- Software
  - Sistema operativo Windows 2000, XP, 2003,2008, Vista o Windows 7 con el último nivel de parche aplicado.
  - .Net Framework 3.5 SP1.
  - MS Chart Controls para .Net Framework 3.5 SP1 (incluida en la instalación de la herramienta).

**Para el servidor de back-end la base de datos:**

- Hardware
    - Compatible con Pentium III o superior 1 GHz o más.
    - 2 GB de memoria RAM.
    - 4 GB de espacio libre en disco.
- Software
    - Sistema operativo Windows 2000, XP, 2003,2008, Vista o Windows 7 con el último nivel de parche aplicado.
    - SQL Server 2005, 2008 o 2008 R2 (Express o superiores) con el último nivel de parche instalado en cualquiera de las versiones.
    - .Net Framework 3.5 SP1
    - MSXML 6.0 (se instala con el producto).
    - Conectividad mediante TCP/IP.

En caso que el cliente y el servidor de la base de datos se instalen en el mismo equipo los requisitos de memoria y disco serían el mayor de los indicados, en tal caso se recomienda la versión Express de MS SQL.

### 6.3.5 FASE DE EVALUACIÓN DEL PROTOTIPO: PLAN DE PRUEBAS

Las pruebas son siempre un proceso vital para cualquier desarrollo y tiene el fin de constatar la calidad del software desarrollado y depurar posibles errores. Por tanto se debe realizar un plan de pruebas que permita verificar que el prototipo cumple con los requisitos determinadas la fase de análisis.

Las pruebas se plantearán cómo un proceso destructivo ya que no se trata demostrar la ausencia de fallos en el desarrollo puesto que la amplitud de todos los escenarios hace imposible la exploración de todos ellos; es decir se podrá decir que una prueba es exitosa siempre y cuando localice un error o una incoherencia.

La metodología de desarrollo Métrica 3 del Ministerio de Administraciones Públicas (ver referencias) define una serie de pruebas que se han de desarrollar para poder realizar unas pruebas con cierta garantía:

- Pruebas Unitarias.
- Pruebas de Integración.
- Pruebas de Sistema.
- Pruebas de implementación.
- Pruebas de aceptación (usabilidad).

Por aplicabilidad con el entorno y limitaciones de tiempo solamente se realizaron las pruebas de Sistema y de aceptación o usabilidad según lo definido en Métrica 3 y concretamente en el interfaz de aseguramiento de la calidad. A continuación se detalla el plan de pruebas.

#### 6.3.5.1 Pruebas de aceptación

Las pruebas de aceptación están dirigidas a validar que el sistema cumple los requisitos de funcionamiento esperado recogidos en el catálogo de requisitos y en los criterios de aceptación del sistema de información, y conseguir la aceptación final del sistema por parte del usuario. Las pruebas de aceptación buscan la identificación y cumplimiento de los requisitos determinados en el documento de análisis

- Pruebas de requisitos funcionales relacionados con la Gestión de estándares.
- Pruebas de requisitos de seguimiento de los controles definidos en los estándares.
- Pruebas de requisitos de registro de auditorías realizadas y seguimiento de incumplimientos/observaciones.
- Pruebas de requisitos de gestión documental.
- Pruebas de requisitos de definición y seguimiento de métricas.
- Pruebas de requisitos de generación de informes de seguimiento.
- Pruebas de requisitos de generación de gráficas de seguimiento.
- Pruebas de requisitos de gestión de plan de proyectos.
- Pruebas de los restantes requisitos funcionales y no funcionales de índole general (soporte multiorganización, seguridad, concurrencia…etc.).

#### 6.3.5.2 Pruebas del sistema

Las pruebas del sistema son pruebas de integración del sistema de información completo, y permiten probar el sistema en su conjunto y con otros sistemas con los que se relaciona para verificar que las especificaciones funcionales y técnicas se cumplen. Mediante pruebas del conjunto del sistema y de caja negra en el uso de formularios de introducción de datos, informes y gráficas.

Las pruebas de sistema buscan comprobar que la totalidad de los módulos de la herramienta se comportan de la manera esperada, cooperando entre si de manera coherente y compacta.
Se divide en dos tipos de pruebas, pruebas de funcionalidad del sistema y pruebas de caja negra.

Se definen a continuación los formularios donde se realizarán ambos tipos de pruebas que están definidas más adelante.

<u>Ámbito 1: Formularios de Gestión de la Normativa</u>

1. Formulario de Gestión de Normativas.
2. Formulario de Estado de Normativa.
3. Formulario de Evolución de Normativa.

4. Formulario de Gráficos e Informes de la Normativa.
5. Formulario de Comparativa de Evolución de Controles.
6. Formulario de Comparativa de Evolución de Verificaciones.
7. Formulario de Gestión de Revisiones del Control.
8. Formulario de Modificación de Revisión de Control.
9. Formulario de Introducción de Comentarios de la Revisión del Control.
10. Formulario de Gestión de Procedimientos de Comprobación.
11. Formulario de Gestión de Resultados de Procedimiento.
12. Formulario de Gestión de Verificaciones.
13. Formulario de Resultado de Procedimiento.
14. Formulario de Importación de Resultados de Procedimientos.

Ámbito 2: Formularios de Gestión de poblaciones

1. Formulario de Gestión de Poblaciones.

Ámbito 3: Formularios de Gestión de documentos

1. Formulario de Gestión de Documentos.
2. Formulario de Estado de Documentos.

Ámbito 4: Formularios de Gestión de auditorías

1. Formulario de Resumen de Estado de Auditorias.
2. Formulario de Gestión de Auditorias.
3. Formulario de Gestión de Hechos Observados.
4. Formulario de Introducción de Comentarios del Hecho Observado

Ámbito 5: Formularios de Gestión de métricas

1. Formulario de Gestión Métricas.
2. Formulario de Gestión de Resultados de Métricas.

Ámbito 6: Formularios de Gestión de proyectos

1. Formulario de Resumen de Estado de Proyectos.
2. Formulario de Gestión de Proyectos.

Ámbito 7: Formularios de Gestión administrativa de la herramienta

1. Formulario de Resumen de Organizaciones.
2. Formulario de Gestión de Organizaciones.
3. Formulario de Gestión de Departamentos.
4. Formulario de Gestión de Usuarios.
5. Formulario de Modificación de Usuario.

Ámbito 8: Formularios principales y de inicio de sesión

1. Formulario de Inicio.
2. Formulario de Inicio de Sesión.
3. Formulario de Menú de Principal.

Ámbito 9: Otros formularios

1. Formulario AcercaDe.
2. Formulario de Dialogo de Introducción de Fechas para consultas.

#### 6.3.5.2.1 PRUEBAS DE FUNCIONALIDAD DEL SISTEMA

Se comprobará que las funcionalidades en los formularios son las adecuadas, que las funcionalidades que aportan se encuentran agrupadas y accesibles por el usuario de manera similar en toda la aplicación. También comprobará también que el modo de implantación de esas funcionalidades es correcto y lógico con el objetivo buscado y que la integración de los formularios es coherente.

Los códigos de las comprobaciones son los siguientes:

- PP-PSFS-XX para el plan de pruebas de funcionalidad del sistema, siendo XX el código de la comprobación.

Las pruebas a realizar en este punto serán las siguientes:

**PP-PSFS-1** Comprobar que la presentación de los datos es correcta y coherente en la totalidad de la aplicación.

**PP-PSFS-2** Comprobar que los datos una vez introducidos en alta o modificación se visualizan de manera correcta y que los datos se refrescan de manera coherente una vez modificados.

**PP-PSFS-3** Comprobar que la cancelación en medio de una introducción de datos no causa errores de integridad en los datos.

**PP-PSFS-4** Comprobar que la navegación por la herramienta es coherente. Intentar forzar errores modificando el tamaño de las ventanas de los formularios o cerrándolas sin seguir el flujo previsto.

**PP-PSFS-5** Comprobar que las ayudas en pantalla son correctas y coherentes con el contexto en el que se presentan.

**PP-PSFS-6** Comprobar posibles faltas de ortografía o gramaticales en los textos presentados en pantalla (excluyendo los datos introducidos por el usuario.

**PP-PSFS-7** Comprobar que no se visualizan datos internos de la aplicación o que no sean de utilidad al usuario.

**PP-PSFS-8** Comprobar que los elementos del interfaz de usuario cómo iconos, menús, botones, tipos de letra…etc. Presentan una apariencia uniforme en todos los formularios de la herramienta. (Por ejemplo que el icono de salida del formulario es similar en todos los formularios de la herramienta).

**PP-PSFS-9** Comprobar que los errores están controlados y que en caso que se produzcan no causan incoherencia, corrupción o falta de integridad en los datos de la herramienta. Comprobar así mismo que los mensajes de descripción del error son entendibles y útiles para el usuario.

**PP-PSFS-10** Comprobar la usabilidad de la aplicación con distintas resoluciones de pantalla.

#### 6.3.5.2.2 PRUEBAS DE CAJA NEGRA

Así mismo se realizarán pruebas de caja negra que buscan determinar que cada formulario cumpla con su funcionalidad sin necesitad de internarnos en su estructura interna, es decir habrá que comprobar que las salidas al usuario sean las correctas y esperadas según las entradas y que los datos introducidos guardan la integridad deseada.

Para la realización de estas pruebas se diseñaran tres tipos de pruebas: Tipo A, B y C. El tipo A consiste en introducir datos correctos, la B en introducir datos que estén en el límite de los rangos permitidos y por último la C introduce datos no válidos.

##### 6.3.5.2.2.1 Pruebas tipo A

Para cada elemento del formulario se introducirán los datos solicitados por la herramienta, poniendo especial cuidado que se ajusten con lo esperado por la herramienta y se comprobará que la herramienta se comporta de la manera expuesta en la funcionalidad que se está utilizando.

Comprobar los siguientes elementos que admiten la entrada de datos:

- Cajas de texto:
  - Texto normal sin acentos, comillas o símbolos de otro tipo.
  - Texto nulo donde esté permitido.
- Cajas de selección: Los valores permitidos.
- Cajas de fechas: Los valores presentados y permitidos.
- Cajas de selección de archivos de importación de datos XML: Archivos existentes y bien formados.
- Celdas de selección: Selección de celdas con contenido.
- Selección de botones activos.

##### 6.3.5.2.2.2 Pruebas tipo B

Para cada elemento del formulario se introducirán los datos solicitados por la herramienta, poniendo especial cuidado que sean valores extremos a lo esperado por la herramienta y se comprobará que la herramienta se comporta de la manera expuesta en la funcionalidad que se está utilizando.

Introducción de datos en el límite:

- Cajas de texto:
    - Texto normal con acentos, comillas o símbolos de todo tipo y caracteres de escape. Introducir valores de cadena de texto extremadamente grandes o nulos donde se supone se permita.
    - En caso de valores se introducirán valores cero o nulos, valores negativos y valores extremadamente grandes.
- Cajas de fechas: Fechas extremas en un pasado o futuro lejano.
- Cajas de selección de archivos de importación de datos XML: Archivos existentes bien formados pero extremadamente grandes y asociados a procedimientos con valor cero.
- Selección de botones que no deberían estar activos.
- Comprobar en caso de conseguir introducir estos valores que son visualizados correctamente en los generadores de gráficas e informes.

#### 6.3.5.2.2.3 Pruebas tipo C

Para cada elemento del formulario se introducirán los datos solicitados por la herramienta, poniendo especial cuidado que sean valores prohibidos o no permitidos a lo esperado por la herramienta y se comprobará que la herramienta se comporta de la manera expuesta en la funcionalidad que se está utilizando, controlando el error y evitando poner en riesgo la integridad de los datos.

Para cada elemento del formulario se introducirán los datos esperados:

- Cajas de texto:
    - Texto nulo donde no esté permitido.
    - Tipo de datos que no se corresponden con lo esperado (p.e. caracteres donde se espera número).
- Cajas de selección: Los valores no permitidos.
- Cajas de fechas: Los valores no presentados y no válidos (fechas inexistentes).
- Cajas de selección de archivos de importación de datos XML: Archivos no existentes y archivos malformados o binarios.
- Celdas de selección: Selección de celdas sin contenido.
- Selección de botones inactivos.
- Comprobar en caso de conseguir introducir estos valores que son visualizados correctamente en los generadores de gráficas e informes.

### 6.3.5.3 Resultado de la fase de evaluación y pruebas

No se expondrán los resultados detallados de la fase dada su amplitud, sin embargo se expondrá a modo de resumen las conclusiones finales:

- Las pruebas de aceptación se cumplieron de manera general, ningún requisito funcional importante no cumplió las expectativas de manera general en el prototipo inicial.

- Los requisitos no funcionales como seguridad, concurrencia...etc., quedaron cumplidos en su mayoría por la arquitectura utilizada (SQL Server, VB .Net).
- Las pruebas de sistema destaparon múltiples fallos, sobre todo relativos a errores en la introducción de datos del usuario y datos límite que fueron corregidos progresivamente en prototipos sucesivos para mejorar la experiencia y sensación de calidad del usuario en la herramienta.

## 6.3.6 FASE DE MEJORA DEL PROTOTIPO

En esta fase se recogen mejoras propuestas por los usuarios/clientes, una vez se estudia la posibilidad de su implantación en la herramienta y se inicia un nuevo ciclo de la metodología de desarrollo para el nuevo prototipo.

### 6.3.6.1 Mejoras incorporadas desde versiones anteriores

A modo de ejemplo se presentan las mejoras detectadas por el cliente o bien por el equipo desarrollo e incorporadas desde versiones anteriores de la herramienta y presentes en la versión actual (Versión 1.40).

- **Mejoras en la gestión de normativas:**
  - Cambios en la importación de normativas: La herramienta debe permitir importar los procedimientos de verificación en el mismo archivo XML.
  - Se cambiarán las normativas desarrolladas para que incluyan procedimientos de verificación genéricos.
  - Se permite al usuario la opción de utilizar los procedimientos genéricos en la asignación de una normativa la organización en caso que la normativa asignada cuente con ellos.
  - Se permite al usuario exportar normativas en el formato XML de importación.
  - Mejoras en la validación de archivos XML y en la información devuelta al usuario en caso de error.
- **Mejoras en gráficos de estado**
  - Cambios en los formularios de navegación de los gráficos de estado y comparativas de las normativas: Ahora se hace en un único formulario y las diferentes gráficas están accesibles través de un menú contextual.
- **Mejoras en Informes:**
  - Se modifica informe de estado de verificaciones y procedimientos de comprobación para que incluya el último estado de las verificaciones y el último resultados del procedimiento.
- **Mejoras en la implantación de normativas**
  - Se presenta al usuario la valoración del estado de madurez del control mediante un porcentaje numérico.
- **Mejoras la gestión en verificaciones:**
  - Incluir los estados de verificaciones que tengan en cuenta los procedimientos sin resultados.

- Nuevos estados en las verificaciones que tienen en cuentas aquellos casos de procedimientos sin resultados.

- **Mejoras en gestión de contactos:**
  - Se permite la gestión de contactos que permitirá al usuario enviar correos electrónicos (manualmente).
- **Mejoras en gestión de proyectos:**
  - Nueva opción para visualizar la evolución del proyecto.
  - Información al usuario sobre el tiempo transcurrido y la valoración del porcentaje completado desde el inicio del proyecto hasta el cierre en proyectos cerrados o hasta la fecha actual en proyectos activos.
  - Se actualiza el estado de proyecto a la fecha real de inicio del mismo en caso de modificación de las verificaciones que componen el proyecto.
- **Mejoras en el interfaz de usuario**
  - Cambios y mejoras en la uniformidad del aspecto y la usabilidad (colores, tipo de letra...etc.) de los formularios y de los informes.
  - Reorganizado el menú principal en categorías para hacerlo más coherente con los casos de uso.
  - Nuevo interfaz de configuración que permite modificar la configuración relativa al repositorio de datos utilizado por la herramienta sin necesidad de editar manualmente el archivo XML de configuración.
  - Mejoras en la ayuda contextual: Se incluye un archivo de ayuda en línea de Windows con el mismo contenido del manual de usuario de la versión 1.4.
- **Mejoras en rendimiento y depuración de errores**
  - Mejorada la eficiencia en consultas de la base de datos.

#### 6.3.6.2 Mejoras propuestas para versiones futuras

En este apartado se presentan las mejoras propuestas para versiones sucesivas de la herramienta, sobresaliendo de manera especial la integración con la herramienta PILAR y la racionalización de los marcos normativos.

- **Integración con la herramienta de análisis de riesgos PILAR**
  - Posibilidad de importar datos obtenidos desde PILAR referidos a los riesgos con objeto de dar una serie de métricas y guardarlas como valores históricos de referencia.
  - Posibilidad de exportar los datos de evaluación de los controles ISO 27002 al formato de PILAR para importarlos es esta herramienta.
- **Mejoras en la Gestión de activos/poblaciones**
  - Explotar la información relacionada con los activos/poblaciones definidas, permitiendo ver los resultados de los procedimientos de verificación que se han particularizado para cada población.

- Mejorar la definición de activos/poblaciones, pudiendo recoger una serie de datos adicionales a los ya existentes como son:
    - Propietario
    - Custodio.
    - Importancia (Alta, Media, Baja).
    - Tipología del activo (Tipificar).

- **Mejoras en la Gestión documental**
    - Presentar el grado de implantación de los documentos, a través del apartado de Gestión documental, de acuerdo al nivel de implantación de los procedimientos relacionados.
    - Posibilidad de visualizar la evolución del estado de los documentos mediante un histórico de la evolución del marco normativo y documental de la organización.
- **Mejoras en la Gestión de perfiles**
    - Introducción de nuevos perfiles como:
        - Auditor: Perfil de sólo lectura
        - Informes: Solo acceso a los informes.
- **Mejoras en la gestión de Normativas y controles**
    - Racionalización de controles, a través de un marco unificado y personalizado de controles basado en otras normativas estándares.
    - Posibilidad de mostrar el nivel de cumplimiento de cada capítulo de una norma y el porcentaje de cumplimiento general de dicha norma que se alcanzará tras la ejecución de un proyecto. Serían datos informativos, no sería necesario que quedaran registrados en la herramienta.
    - Interfaz gráfico de definición interactiva de repositorios de controles.
- **Mejoras en la gestión de proyectos**
    - Dar valoración del grado de avance de los proyectos a nivel de control.
    - Listado/Informe de los proyectos.
- **Otro tipo de mejoras internas**
    - Cambios y mejoras en la estructura interna de las clases de la herramienta.
    - Cambios internos orientados a permitir en un futuro múltiples organizaciones por usuario.

# 7. CONCLUSIONES

Una vez se ha descrito el proceso de implantación de un SGSI que permite la gestión de la seguridad en una organización y finalizado el proceso de desarrollo la herramienta HIS-SGSI se implantó en un primer cliente al que se le suministraron prototipos sucesivos que arreglaban los fallos detectados y que cubrían nuevos requisitos o extendían los existente.

Este primer cliente sigue utilizando la herramienta a día de hoy como herramienta de soporte en sus procesos internos de gestión de la seguridad.

Por ejemplo con el soporte de la herramienta tras su implantación se aprecia la mejora del nivel de seguridad en la organización, se puede ver en las gráficas comparativas del nivel de la madurez de la implantación de los controles entre enero de 2010 y enero de 2013.

Como se aprecia en los gráficos de radar de comparativa del estado de los controles por capítulo algunos capítulos de ISO 27002, no varían aunque otros mejoran hasta en un 10%, siendo la media de evolución de un 3%.

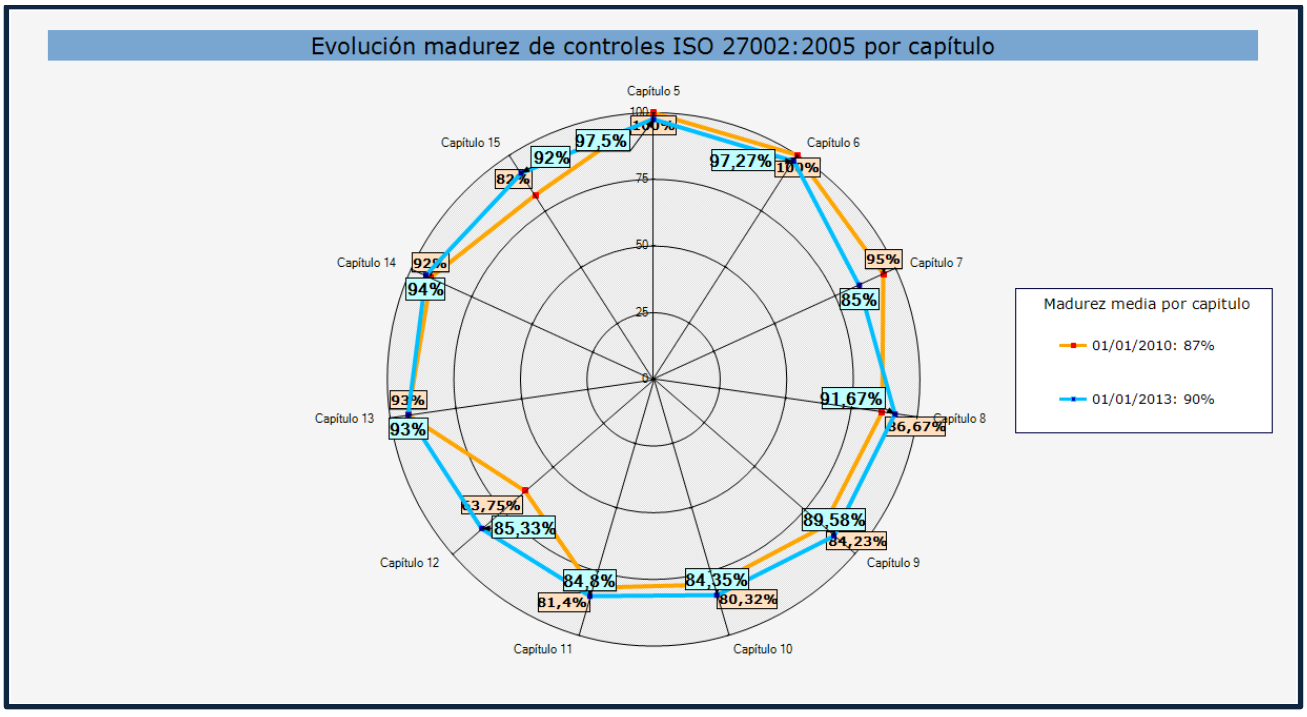



**Ilustración 32. Evolución del nivel de madurez de los controles ISO 27002 por capítulo**

La distribución estado de madurez de los controles también mejora sustancialmente, especialmente en los controles no revisados y definidos.

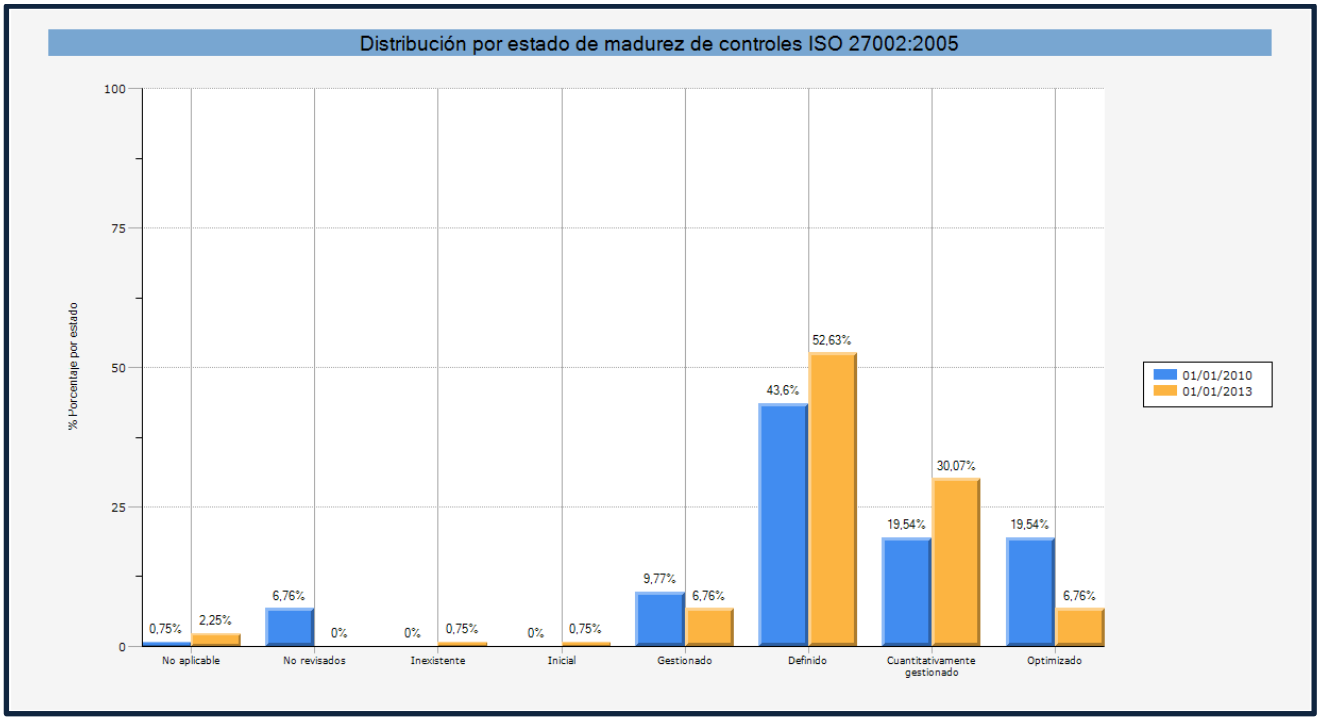



**Ilustración 33. Distribución de estados del nivel de madurez de los controles**

La mejora de los procedimientos de verificación, que pasan en su mayoría de no ser verificables a estar parcial o completamente implementados.

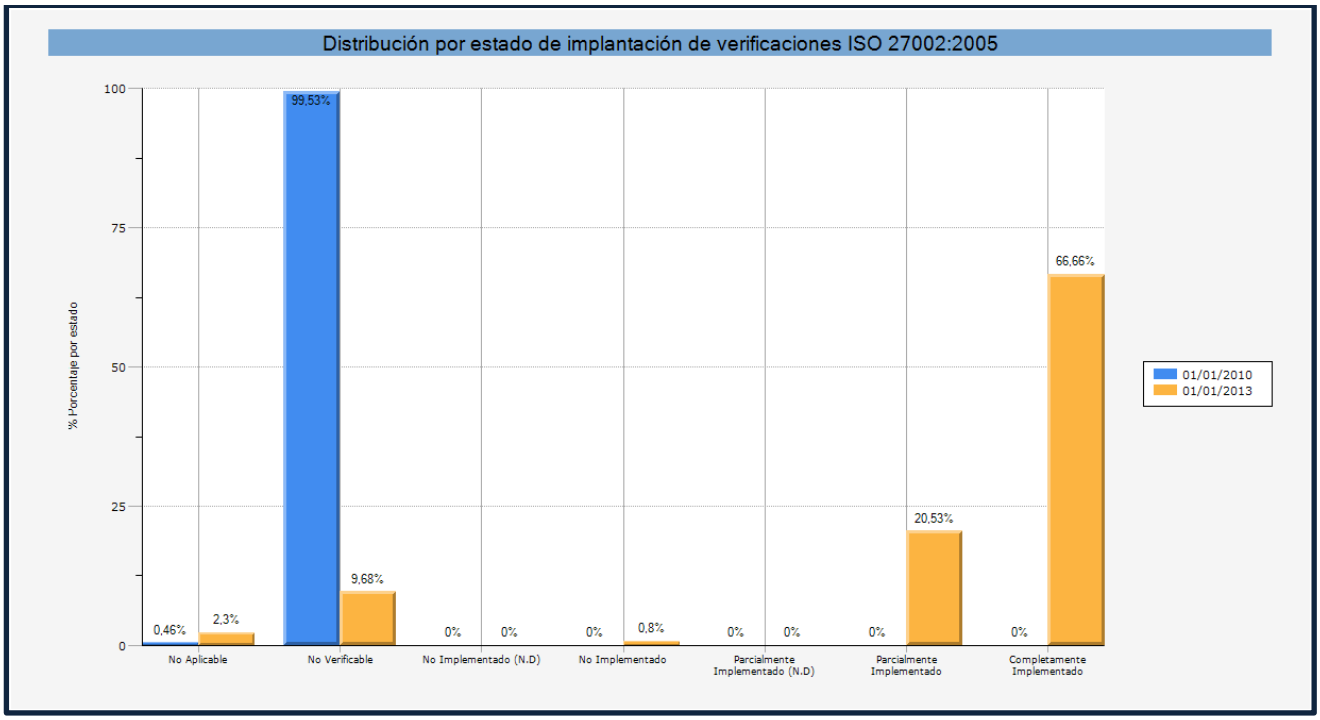



**Ilustración 34. Distribución del estado de implantación de los procedimientos de verificación**

Igualmente en la distribución de las verificaciones por capítulo se aprecia la mejora ya que la mayoría de no ser verificables a estar parcial o completamente implementados.

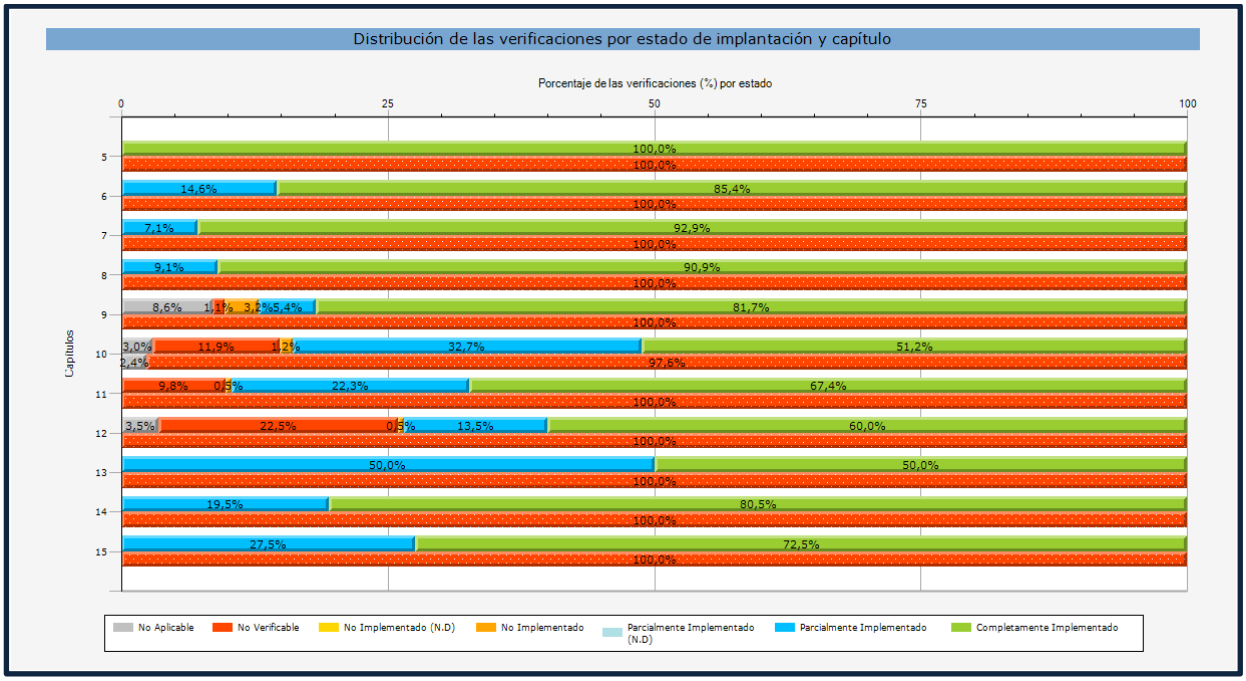



**Ilustración 35. Distribución del estado de implantación de los procedimientos de verificación por capítulo**

La herramienta también se encuentra funcional en varios clientes reales que comentaremos de manera general y sin determinar sus identidades.

- **Cliente 1**: Administración General del Estado Español. Inicialmente la herramienta se desarrolló para un ministerio y actualmente se encuentra activa en las oficinas de seguridad de tres Ministerios del Gobierno Español.
- **Cliente 2:** Utilizada en dos entidades bancarias a nivel nacional como soporte en la gestión de la seguridad de los departamentos de seguridad de la información.
- **Cliente 3:** Utilizada en una consultora nacional como herramienta interna de soporte en la obtención de la certificación de ISO 27001.
- **Cliente 4:** Utilizada en una mutualidad de salud. Utilizada como soporte en la Oficina de Seguridad en la gestión de la seguridad.

**Por todo lo anterior se puede afirmar que la herramienta HIS-SGSI ha sido un caso éxito tanto como utilidad de soporte en la implantación de un SGSI en la organización en la que se implementó como de la metodología de desarrollo expuesta anteriormente y del equipo de desarrollo.**

# 8. BIBLIOGRAFÍA Y REFERENCIAS


**ISO - International Standards Office**

- ISO/IEC 27001:2005, *Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI).* ISO/IEC 2005
- ISO/IEC 27002:2005, *Tecnología de la información. Técnicas de seguridad. Código de buenas prácticas de la Gestión de la Seguridad de la Información*. ISO/IEC 2005.
- ISO/IEC 27004:2009, *Tecnología de la información. Técnicas de seguridad. Gestión de Seguridad de la Información. Métricas*. ISO/IEC 2009.
- ISO/IEC 27005:2008, *Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de Seguridad de la Información*. ISO/IEC 2008
- ISO/IEC *21827:2002, Tecnología de la Información – Técnicas de seguridad – Ingeniería de Seguridad de Sistemas – Modelo de Madurez de Capacidades (SSE-CMM)*. ISO/IEC 2002
- ISO/IEC *Guía 73:2005, Gestión del riesgo. Vocabulario. Directrices para la utilización de las normas*. ISO/IEC 2005.

**AENOR – Asociación Española de Normalización y Certificación (http://www.aenor.es)**

- UNE 71501 *Tecnología de la Información (TI). Guía para la gestión de la seguridad de TI*. AENOR 2001.
- UNE 71502 *Tecnología de la Información (TI). Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI),* AENOR, 2004.
- UNE 71504 *Tecnología de la Información (TI). Metodología de análisis y gestión de riesgos para los sistemas de información*, AENOR, 2008.

**BSI – British Standards Institution**

- BS 7799-3:2006 *Information Security Management Systems. Guidelines for information Security Risk Management.* BSI 2006.

**ENS- Esquema Nacional de Seguridad**

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. BOE Viernes 29 de enero de 2010

**MAGERIT**

- F. López, M.A. Amutio, J. Candau y J.A. Mañas. *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, versión 2*. Ministerio de Administraciones Públicas, 2006. Disponible en: http://publicaciones.administracion.es

**METRICA 3**

- *Metodología de Planificación, Desarrollo y Mantenimiento de sistemas de información versión 3.* Ministerio de Hacienda y Administraciones Públicas. Disponible en: http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=P80029225129365155099 1&langPae=es&detalleLista=PAE_000000432

**NIST – National Institute of Standards and Technology (http://www.nist.gov)**

- NIST *SP 800-30, Risk Management Guide for Information Technology Systems*. NIST Special Publication, 2002.
- NIST SP 800-12. *An Introduction to Computer Security: the NIST Handbook*. NIST Special Publication, 1995.

**Seguridad de la información:**

- *Official (ISC). Guide to the CISSP Exam*. S. Hansche, J. Berti, C. Hare. (ISC)2. 2004.
- *CISSP Exam Guide: All In One 3rd Edition*. S. Harris. McGraw-Hill/Osborne, 2006.

**The Internet Engineering Task Force (IETF)**

- RFC 2196 *Site Security Handbook*. Disponible *en:* <http://www.ietf.org/>

**Proyecto Fin de Carrera/Grado**

- J.M Matalobos Veiga, J. Carrillo Verdún. *Análisis de riesgos de seguridad de la información*. Archivo Digital UPM. 2009.

**Metodología de desarrollo de prototipos sucesivos**

- Nielsen, J. *Usability Engineering*. Boston Academic Press, 1993

**Metodología de estimación por casos de uso (Use Case Points)**

- Cockburn, Alistair. *Writing Effective Use Cases*. Addison-Wesley, 2001. Disponible en: http://alistair.cockburn.us/get/2465
- Ribu, Kirsten. *Estimating Object-Oriented Software Projects with Use Cases*. Master of Science Thesis. University of Oslo, Department of Informatics. 2001. Disponible en: http://www.bfpug.com.br/Artigos/UCP/Ribu-Estimating_O-O_SW_Projects_with_Use_Cases.pdf
- Gómez, Julián. *Método de Estimación Puntos Casos de Uso (Use Case Points).* 14 de Febrero de 2013. Disponible en: http://www.laboratorioti.com/2013/02/14/metodo-de-estimacion-puntos-casos-de-uso-use-case-points/
- Cohn, Mike. *Estimating with Use Case Points*. Disponible en: http://www.cs.cmu.edu/~jhm/Readings/Cohn%20-%20Estimating%20with%20Use%20Case%20Points_v2%2012-24-50-761.pdf

# 9. GLOSARIO

## 9.1 Glosario de términos

En este glosario se presentan los términos de uso frecuente en el entorno del análisis de riesgos. Junto a la definición de cada término se ha introducido la traducción al inglés, para facilitar la comprensión de la literatura técnica escrita en ese idioma.

En la elaboración de este glosario se han tenido en cuenta las definiciones recogidas en los principales estándares que se detallan en el apartado de Estado de la Cuestión. Para cada término se ha seleccionado el que se ha considerado más adecuado en el contexto del proyecto, y en algunas entradas se ha preparado una nueva definición que se ha considerado más apropiada para este entorno.

- **Aceptación** (Aceptation): Estrategia de gestión de riesgos que consiste en la aceptación del nivel de riesgo actual. Puede seleccionarse automáticamente si el nivel de riesgo es inferior al umbral de riesgo considerado tolerable o tras un análisis coste/beneficio considerando las alternativas disponibles para reducir o eliminar un riesgo superior.
- **Activo** (Asset): Cualquier elemento valioso o necesario para que la organización cumpla sus objetivos. Cfr.
- **Activo de información** (Information asset): Cualquier información valiosa o necesaria para que la organización cumpla sus objetivos.
- **Acuerdo de nivel de servicio** (Service level agreement): Acuerdo entre dos partes en relación a las características mínimas exigibles a un servicio prestado entre ellas.
- **Amenaza** (Threat): Causa potencial de un incidente que puede resultar en un daño a un sistema o a una organización.
- **Análisis cualitativo** (Qualitative analysis): Análisis basado en el uso de escalas de valoración.
- **Análisis cuantitativo** (Quantitative analysis): Análisis basado en cuantificación numérica de magnitudes, generalmente en términos económicos.
- **Análisis de impacto sobre el negocio** (Impact analysis): Estudio de las consecuencias que tendría la realización de una determinada amenaza sobre la organización.
- **Análisis de riesgos** (Risk analysis, risk assessment): Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización.
- **Análisis mixto** (Mixed analysis): Análisis que emplea una combinación de términos cuantitativos y cualitativos.
- **Ataque** (Attack): Amenaza de origen intencionado.
- **Ataque de día cero** (Zero day attack): Ataque que se produce antes de la publicación de la vulnerabilidad que explota.

- **Autenticidad** (Authenticity): Propiedad que asegura que la identidad de un elemento o recurso es la que se le supone. La autenticidad aplica a elementos como usuarios, procesos, sistemas e información.
- **Ciclo de Deming** (PDCA cycle): Ver ciclo de mejora continua.
- **Ciclo de mejora continua** (PDCA cycle): Herramienta de gestión para la evolución de los procesos que define cuatro fases (planificación, ejecución, comprobación, actuación).
- **Concienciació**n (Awareness): Conjunto de medidas definidas para que las personas relacionadas con la organización (personal, personal subcontratado, clientes, proveedores, etc.) conozcan los riesgos de seguridad y los controles que pueden y deben aplicar para colaborar en su mitigación.
- **Confidencialidad** (Confidentiality): Propiedad de que la información no está disponible ni es divulgada a personas, procesos o dispositivos no autorizados.
- **Control** (Control): Ver salvaguarda.
- **Control correctivo** (Corrective control): Control definido para reducir o eliminar el impacto de incidente de seguridad ocurrido.
- **Control detectivo** (Detective control): Control definido para detectar la ocurrencia de un incidente de seguridad y permitir la reacción ante el mismo.
- **Control disuasorio** (Dissuasive control): Control preventivo definido para hacer desistir a un potencial atacante antes de que se produzca el ataque.
- **Control mitigante** (Mitigating control): Control definido para suplir las deficiencias de otro control.
- **Control preventivo** (Preventive control): Control definido para dificultar o impedir la ocurrencia de un incidente de seguridad.
- **Declaración de aplicabilidad** (Statement Of Applicability, SOA): Documento formal en el que, para un conjunto de salvaguardas, se indica sin son o no de aplicación en el sistema de información bajo estudio.
- **Degradación** (Degradation): Pérdida del valor de un activo como consecuencia de la realización de una amenaza.
- **Disponibilidad** (Availability): Propiedad de que la información y sus activos asociados sea accesible y utilizable bajo la demanda por una entidad autorizada.
- **Efectividad** (Effectiveness): Ver eficacia.
- **Eficacia** (Effectiveness): Propiedad de que se cumplen todos los objetivos de negocio definidos para un determinado elemento.
- **Eficiencia** (Efficiency): Propiedad de que un requisito de negocio se alcanza realizando un consumo óptimo de los recursos disponibles para ello.
- **Escenario de riesgos** (Risk scenario): Descripción del efecto de un conjunto determinado de amenazas sobre un determinado conjunto de activos, recursos y salvaguardas, teniendo en cuenta determinadas hipótesis definidas.

- **Estimación de riesgos** (Risk estimation): Proceso utilizado para asignar valores de probabilidad e impacto asociados a un riesgo.
- **Evaluación de riesgos** (Risk evaluation): Comparación del riesgo estimado contra un determinado criterio para determinar su significatividad.
- **Evaluación de salvaguardas** (Safeguard assessment): Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que mitigan.
- **Fiabilidad** (Reliability): Propiedad de mantener de forma consistente un comportamiento y unos resultados.
- **Frecuencia** (Frecuency): Tasa de ocurrencia de una amenaza.
- **Gestión de riesgos** (Risk management, risk treatment): Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.
- **Grupo Especial de Ingeniería de Internet** (Internet Engineering Task Force (IETF)) Organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento y seguridad.
- **Impacto** (Impact): Consecuencia potencial que sobre un activo tiene la realización de una amenaza.
- **Impacto residual** (Residual Impact): Consecuencia potencial que sobre un activo tiene la realización de una amenaza, una vez considerados los efectos mitigantes de las salvaguardas implantadas.
- **Incidente** (Incident): Evento inesperado o indeseado que puede causar un compromiso de la seguridad de la información y de las actividades de negocio.
- **Indicador de seguridad:** Valor que se obtiene comparando datos o atributos lógicamente relacionados, referentes al comportamiento de una actividad, proceso o control, dentro de un tiempo específico.
- **Integridad** (Integrity): Propiedad que asegura que la información y los métodos de procesamiento sean exactos y completos.
- **Línea base de controles** (Controls baseline): Conjunto mínimo de salvaguardas definido para un sistema u organización.
- **Mapa de riesgos** (Risk map): Relación de las amenazas valoradas a las que están expuestos los activos.
- **Medida de seguridad:** Salvaguarda.
- **Métrica de seguridad** (Metric)**:** Conjunto de preceptos y reglas, necesarios para poder medir de forma real el nivel de seguridad de una organización.
- **No repudio** (Non repudiation): Propiedad de que un elemento que ha realizado una determinada acción en el sistema no puede negar su realización.
- **Normativa de seguridad** (Security regulation): Conjunto de documentos que desarrollan la política de seguridad.

- **Objetivo de punto de recuperación** (Recovery Point Objective): Punto en tiempo en el que un determinado proceso se recupera tras un incidente. Determina el volumen tolerable de transacciones que puede perderse en caso de un incidente.
- **Objetivo de tiempo de recuperación** (Recovery Time Objective): Periodo de tiempo objetivo definido para recuperar el funcionamiento de un determinado proceso tras un incidente.
- **Organización:** Entidad con estructura y jerarquías definidos y con un objetivo establecido que intenta alcanzar a través del desempeño de una serie de actividades. Tipos de organizaciones pueden incluir industrias, empresas comerciales y de servicios, organizaciones militares y gubernamentales y cualquier tipo de instituciones públicas y privadas.
- **Pérdida esperada** (Single loss expectancy): Pérdidas estimadas por la realización de una determinada amenaza sobre un recurso de información.
- **Plan de continuidad de negocio** (Business continuity plan): Colección documentada de procedimientos e información desarrollada, recopilada y mantenida de modo que esté disponible para su uso en caso de incidentes y permita a la organización continuar la ejecución de sus actividades críticas a un nivel aceptable predefinido.
- **Plan de recuperación ante desastres** (Disaster recovery plan): Conjunto de medidas definidas para recuperar un determinado servicio de soporte al negocio tras una interrupción provocada por un incidente.
- **Plan de seguridad** (Security plan): Conjunto de proyectos de seguridad priorizados y presupuestados que permiten materializar las decisiones de gestión de riesgos.
- **Política de seguridad** (Security policy): Conjunto de reglas, directivas y prácticas que gobiernan cómo se gestionan, protegen los activos y recursos de información.
- **Probabilidad** (Likelihood): Medida de expectativa de que una amenaza se realice en un periodo de tiempo determinado, generalmente un año.
- **Proceso de gestión de la seguridad** (Security Management process): Conjunto de objetivos, recursos, funciones, responsabilidades y tareas definidos para garantizar la seguridad de una organización.
- **Proyecto de seguridad** (Security project): Conjunto de actividades interrelacionadas definidas para lograr un determinado objetivo en relación a la mejora o mantenimiento del nivel de seguridad de la información.
- **Recurso de información** (Information resource): Cualquier elemento empleado en el tratamiento de activos de información.
- **Reducción** (Reduction): Estrategia de gestión de riesgos que consiste en la aplicación de salvaguardas para reducir un riesgo cuyo nivel supera el umbral de riesgo tolerable definido.
- **Requisito de seguridad** (Security requirement): Conjunto de propiedades de la información y sus recursos cuyo incumplimiento supone un incidente que tiene como consecuencia un daño para un sistema o la organización.

- **Riesgo** (Risk): Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.
- **Riesgo acumulado** (Accumulated Risk): Riesgo calculado tomando en consideración el valor propio de un recurso de información y el valor de los activos de información que dependen de él. Este valor se combina con la degradación y la frecuencia de las amenazas del recurso de información considerado.
- **Riesgo efectivo** (Effective Risk): Riesgo remanente en el sistema tras la valoración de las salvaguardas actualmente implantadas.
- **Riesgo intrínseco** (Intrinsic Risk): Riesgo en el sistema sin valorar la eficacia de las salvaguardas implantadas o incluidas en el plan de seguridad.
- **Riesgo repercutido** (Affected Risk): Riesgo calculado tomando en consideración únicamente el valor propio de un activo de un activo de información. Este valor se combina con la degradación y la frecuencia de las amenazas de los recursos de información de los que depende.
- **Riesgo residual** (Residual Risk): Riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información.
- **Salvaguarda** (Safeguard): Medida establecida para la reducción del riesgo.
- **Seguridad** (Security): Capacidad de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que pueden causar un daño a un sistema o a la organización.
- **Seguridad de la información** (Information Security): Capacidad de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que pueden causar un daño a los activos de información de una organización.
- **Seguridad informática** (IT Security): Capacidad de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que pueden causar un daño a los recursos de información tecnológicos de una organización.
- **Sistema de gestión de seguridad de la información** (Information Security Management System): Herramienta a disposición de la Dirección de las organizaciones para llevar a cabo las políticas y los objetivos de seguridad. Comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información. Está basado en el ciclo de la mejora continua (PDCA).
- **Tolerancia al riesgo** (Risk tolerance): Cantidad de riesgo que una organización es capaz de gestionar.
- **Transferencia** (Transfer): Estrategia de gestión de riesgos que consiste en transferir un riesgo a una entidad externa que deba encargarse de su gestión y que asuma los daños en caso de ocurrencia de un incidente.
- **Trazabilidad** (Accountability): Propiedad de que se puede determinar el elemento que ha realizado una determinada acción en el sistema.

- **Valor** (Value): Estimación de la utilidad de un determinado activo de información para la organización, teniendo en cuenta los diferentes requisitos de seguridad definidos.
- **Valor acumulado** (Accumulated value): Valor de un determinado recurso de información teniendo en cuenta el valor de los activos de información que dependen de él.
- **Vulnerabilidad** (Vulnerability): Debilidad en un recurso de información que puede ser explotada por una amenaza para causar un daño a un sistema o a la organización.

## 9.2 Glosario de abreviaturas

En este glosario se presentan las abreviaturas de uso frecuente en este documento y en el dominio del análisis y la gestión de riesgos de seguridad de la información.

- AGR: Análisis y Gestión de Riesgos.
- ALE (Annual Loss Expectancy): Pérdida anual esperada.
- ARO (Annual Rate of Occurrence): Tasa anual de ocurrencia.
- BCP (Business Continuity Plan): Plan de continuidad de negocio.
- BIA (Business Impact Analysis): Análisis de impacto sobre el negocio.
- BSI (British Standards Institute): Instituto Británico de Estándares.
- CMM (Capability Maturity Model): Modelo de madurez de capacidades.
- CPD: Centro de Proceso de Datos
- DRP (Disaster Recovery Plan): Plan de recuperación de desastres.
- ECF (Environmental Complexity Factor): Factores de complejidad del entorno
- IEC (International Electrotechnical Commission): Comisión Electrotécnica Internacional.
- IETF (Internet Engineering Task Force): Grupo Especial de Ingeniería de Internet.
- ISMS (Information Security Management System): Sistema de gestión de seguridad de la información.
- ISO (International Organization for Standardization): Organización Internacional de Estandarización.
- PCN: Plan de continuidad de negocio.
- PDCA (Plan, Do, Check, Act): Planificar, Ejecutar, Comprobar, Actuar. Ciclo de Deming o de mejora continua.
- PRD: Plan de recuperación de desastres.
- RFC (Request For Comments): Documento de petición de comentarios para la creación de estándares en Internet.
- RPO (Recovery Point Objective): Objetivo de punto de recuperación.
- RTO (Recovery Time Objective): Objetivo de tiempo de recuperación.
- SGSI: Sistema de Gestión de Seguridad de la Información.
- SLA (Service Level Agreement): Acuerdo de nivel de servicio.
- SLE (Single Loss Expectancy): Pérdida esperada.

- SOA (Statement Of Applicability): Declaración de aplicabilidad.
- TCF (Technical Complexity Factor): Factor de complejidad técnica
- TR (Technical Report): Informe técnico.
- UAW (Unadjusted Actor Weight): Factor de peso sin ajustar de los actores.
- UML (Unified Modeling Languaje): Lenguaje de Modelado Unificado.
- UUCW (Unadjusted Use Case Weight): Factor de peso sin ajustar de los casos de uso.

# 10. ANEXO: INVENTARIO DE CONTROLES/SALVAGUARDAS ISO 27002

En este anexo se detallan las salvaguardas incluidas como anexo en ISO 27001 y desarrolladas en ISO 27002.

- **Políticas, normas y procedimientos de Seguridad**
  - 1.1 - Política de seguridad de la información
  - 1.2 - Revisión de la política de seguridad de la información
- **Organización de la Seguridad de la Información**
  - 1.1 - Compromiso de la dirección con la seguridad de la información
  - 1.2 - Coordinación de la seguridad de la información
  - 1.3 - Asignación de las responsabilidades de la seguridad de la información
  - 1.4 - Proceso de la autorización para las instalaciones de tratamiento de la información
  - 1.5 - Acuerdos de confidencialidad
  - 1.6 - Contacto con autoridades
  - 1.7 - Contacto con los grupos de interés especial
  - 1.8 - Revisión independiente de la seguridad de la información
  - 2.1 - Identificación de los riesgos relacionados con externos
  - 2.2 - Abordando la seguridad al tratar con clientes
  - 2.3 - Abordando la seguridad en acuerdos con terceros
- **Control y Gestión de activos**
  - 1.1 - Inventario de activos
  - 1.2 - Propiedad de los activos
  - 1.3 - Uso aceptable de los activos
  - 2.1 - Guías de clasificación
  - 2.2 - Etiquetado y tratamiento de la información
- **Seguridad de Recursos Humanos**
  - 1.1 - Roles y responsabilidades
  - 1.2 - Investigación
  - 1.3 - Términos y condiciones de la ocupación
  - 2.1 - Responsabilidades de la dirección
  - 2.2 - Conocimiento, educación, y entrenamiento en la seguridad de la información
  - 2.3 - Proceso disciplinario
  - 3.1 - Responsabilidades de la terminación
  - 3.2 - Devolución de activos
  - 3.3 - Retirada de los derechos de acceso

- **Seguridad Física y del Ambiente**
  - 1.1 - Perímetro de seguridad física
  - 1.2 - Controles de entrada física
  - 1.3 - Asegurar oficinas, salas, e instalaciones
  - 1.4 - Protección contra amenazas externas y ambientales
  - 1.5 - Trabajo en áreas seguras
  - 1.6 - Acceso público, entrega, y áreas de carga
  - 2.1 - Localización y protección de equipos
  - 2.2 - Mantenimiento de suministros
  - 2.3 - Seguridad del cableado
  - 2.4 - Mantenimiento de los equipos
  - 2.5 - Seguridad de equipos fuera de los locales de la organización
  - 2.6 - Eliminación y re-utilización segura de equipos
  - 2.7 - Extracción de propiedades
- **Gestión de Comunicaciones y Operaciones de los sistemas de información**
  - 1.1 - Procedimientos operacionales documentados
  - 1.2 - Gestión del cambio
  - 1.3 - Segregación de tareas
  - 1.4 - Separación de los entornos de desarrollo, pruebas, e instalaciones operacionales
  - 2.1 - Entrega de servicio
  - 2.2 - Supervisión y revisión de los servicios de terceros
  - 2.3 - Gestión de cambios en servicios de terceros
  - 3.1 - Gestión de capacidades
  - 3.2 - Aceptación de sistemas
  - 4.1 - Controles contra código malicioso
  - 4.2 - Controles contra código móvil
  - 5.1 - Copia de seguridad de la información
  - 6.1 - Controles de red
  - 6.2 - Seguridad de servicios de red
  - 7.1 - Gestión de soportes extraíbles
  - 7.2 - Eliminación de soportes
  - 7.3 - Procedimientos de utilización de la información
  - 7.4 - Seguridad de la documentación de sistemas
  - 8.1 - Procedimientos y políticas de intercambio de información
  - 8.2 - Acuerdos de intercambio
  - 8.3 - Soportes físicos en tránsito

- 8.4 - Mensajería electrónica (Correo Electrónico, EDI, etc.)
- 8.5 - Sistemas de información de negocio
- 9.1 - Comercio electrónico
- 9.2 - Transacciones On-line
- 9.3 - Información pública disponible
- 10.1 - Registros de auditoría
- 10.2 - Monitorización de uso de sistemas
- 10.3 - Protección de información de registros
- 10.4 - Registros de administrador y operadores
- 10.5 - Registro de fallos
- 10.6 - Sincronización de relojes

- **Control de acceso lógico**
  - 1.1 - Política de control de acceso
  - 2.1 - Registro de usuario
  - 2.2 - Gestión de privilegios
  - 2.3 - Gestión de contraseñas de usuarios
  - 2.4 - Revisión de los derechos de usuario
  - 3.1 - Uso de contraseñas
  - 3.2 - Equipo informático de usuario desatendido
  - 3.3 - Política de puesto de trabajo vacío
  - 4.1 - Política de uso de servicios de red
  - 4.2 - Autenticación de usuarios por conexiones externas
  - 4.3 - Identificación de equipos en red
  - 4.4 - Protección de los puertos de diagnóstico remoto
  - 4.5 - Segregación de redes
  - 4.6 - Control de conexión a redes
  - 4.7 - Control de encaminamiento de la red
  - 5.1 - Procedimientos de inicio de sesión segura
  - 5.2 - Identificación y autenticación del usuario
  - 5.3 - Sistema de gestión de contraseñas
  - 5.4 - Uso de las utilidades del sistema
  - 5.5 - Sesiones inactivas
  - 5.6 - Limitación del tiempo de conexión
  - 6.1 - Restricción de acceso a la información
  - 6.2 - Aislamiento de sistemas sensibles
  - 7.1 - Informática móvil
  - 7.2 – Teletrabajo

- **Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información**
    - 1.1 - Análisis y especificación de requisitos de seguridad
    - 2.1 - Validación de los datos de entrada
    - 2.2 - Control del proceso interno
    - 2.3 - Integridad de mensajes
    - 2.4 - Validación de los datos de salida
    - 3.1. - Política de uso de los controles criptográficos
    - 3.2 - Gestión de claves
    - 4.1 - Control del software en producción
    - 4.2 - Protección de los datos de prueba de sistema Análisis de riesgos de Seguridad
    - 4.3 - Control de acceso al código de fuente del programa
    - 5.1 - Procedimientos de control de cambios
    - 5.2 - Revisión técnica de las aplicaciones tras cambios en el sistema operativo
    - 5.3 - Restricciones en cambios de paquetes de software
    - 5.4 - Fuga de información
    - 5.5 - Desarrollo externalizado del software
    - 6.1 - Control de vulnerabilidades técnicas
- **Gestión de los incidentes de seguridad**
    - 1.1 - Comunicación de eventos de seguridad de la información
    - 1.2 - Comunicación de vulnerabilidades
    - 2.1 - Responsabilidades y procedimientos
    - 2.2 - Aprendiendo de las incidencias de seguridad de la información
    - 2.3 - Recogida de pruebas
- **Gestión de la continuidad del negocio**
    - 1.1 - Inclusión de la seguridad de la información en el proceso de la gestión de la continuidad del negocio
    - 1.2 - Continuidad del negocio y valoración del riesgo
    - 1.3 - Desarrollo e implementación de planes de continuidad incluyendo la seguridad de la información
    - 1.4 - Marco de planificación para la continuidad del negocio
    - 1.5 - Prueba, mantenimiento y reevaluación de los planes de continuidad
- **Cumplimiento regulatorio**
    - 1.1 - Identificación de la legislación aplicable
    - 1.2 - Derechos de propiedad intelectual (IPR)
    - 1.3 - Salvaguarda de los registros de la organización
    - 1.4 - Protección de datos de carácter personal y de la intimidad de las personas
    - 1.5 - Evitar el mal uso de los recursos de tratamiento de la información

- 1.6 - Reglamentación de los controles de cifrado
- 2.1 - Cumplimiento con políticas y estándares de seguridad
- 2.2 - Comprobación del cumplimiento técnica
- 3.1 - Controles de auditoría de sistemas de información
- 3.2 - Protección de las herramientas de auditoría de sistemas